POUR L'ÉCOLE
DE LA CONFIANCE

SDET
Schéma Directeur des Espaces numériques de Travail pour l'enseignement scolaire

Annexe opérationnelle - Ensemble annuaire
Cahier des charges de l'annuaire ENT pour le 2nd degré
version 6.1
Avril 2018

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE

Table des matières

Table des illustrations et tableaux

Conventions typographiques

Cette mise en forme indique les recommandations faites à la maîtrise d'ouvrage en charge du projet ENT afin d'adapter le cahier des charges à ses besoins. Il s'agira notamment de compléter ou préciser certaines attentes en fonction de son projet ENT.

Cette mise en forme indique une précision complémentaire sur les principes de ce document. Ces précisions pourront être supprimées du cahier des charges définitif.

1. Introduction

*Le présent document est une des composantes de l'**ensemble annuaire** de l'**annexe opérationnelle** du **SDET**.*

Il constitue un cahier des charges type pour la fourniture d'une solution d'annuaire pour l'ENT pour le second degré.

1.1. Objet du document

La maîtrise d'ouvrage en charge du projet ENT choisira une des deux formulations proposées ci-dessous en fonction de l'objet du document :

Ce document constitue une annexe au cahier des charges de l'ENT. Il définit le cahier des charges de l'annuaire ENT.

Ce document définit le cahier des charges de l'annuaire ENT.

Ce document a été élaboré à partir du cadre générique issu des travaux du ministère en charge de l'Éducation nationale (MEN) et de la Caisse des dépôts et consignations (CDC). Il a été complété par les exigences spécifiques au projet [NOM_PROJET_ENT].

1.2. Plan du document

Ce document est composé des parties suivantes :

- le chapitre 2 présente une vue d'ensemble de l'annuaire ENT et précise ses principes directeurs ;
- le chapitre 3 décrit le contenu de l'annuaire ENT en termes de périmètre couvert, de modèle de sécurité et de caractérisation des personnes ;
- le chapitre 4 décrit le schéma LDAP et le DIT de l'annuaire ENT, et précise comment sont gérés certains objets ou attributs particuliers ;
- le chapitre 5 définit les principes d'architecture de l'annuaire ENT et les options envisageables ;
- le chapitre 6 décrit les services attendus de l'annuaire ENT, notamment en termes de gestion et d'accès ;
- le chapitre 7 définit les exigences attendues de l'annuaire ENT ;
- le chapitre 8 décrit l'organisation et les processus de gestion types de l'annuaire ENT.

1.3. Annexes (documents indépendants)

L'annexe 2 décrit les caractéristiques des personnes et des structures de l'annuaire ENT pour le second degré.

L'annexe 3 définit le schéma LDAP de l'annuaire ENT et les nomenclatures utilisées pour chaque attribut pour le second degré.

Les annexes 4/4bis présentent les modalités d'alimentation de l'annuaire ENT depuis le SI du MEN et depuis d'autres SI externes pour le second degré

L'annexe 5 traite de l'exploitation et l'exploitabilité du service annuaire ENT pour les premier et second degrés.

2. Présentation générale de l'annuaire ENT

2.1. Qu'est-ce que l'annuaire ENT ?

Dans le cadre des espaces numériques de travail de **l'enseignement secondaire**, l'annuaire ENT est l'annuaire des personnes et des structures en relation avec le ministère en charge de l'Éducation nationale, le ministère en charge de l'Agriculture et les collectivités locales. Il comprend notamment les élèves et leurs responsables, les enseignants, les personnels administratifs…

L'annuaire ENT présente la spécificité que certaines personnes peuvent appartenir à plusieurs catégories. Par exemple, un enseignant peut également être parent d'un élève ou encore assurer des fonctions administratives dans un établissement, en tant que chef d'établissement notamment.
L'annuaire ENT peut, s'il ne délègue pas l'authentification à des guichets externes, permettre de gérer une unique identité tout en autorisant le cumul des catégories.

Différents projets d'ENT pour l'enseignement secondaire sont lancés sous le pilotage des collectivités locales et des services déconcentrés de l'État. Chaque projet ENT, et donc **chaque annuaire ENT,** couvre couramment un **périmètre départemental ou régional**, soit les personnes et structures du périmètre concerné.

Le **responsable de traitement** des données de l'annuaire sur le périmètre de son établissement est le « chef d'établissement » (article 5 de l'arrêté du 13 octobre 2017[1] modifiant l'arrêté du 30 novembre 2006 portant création, au sein du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, d'un traitement de données à caractère personnel relatif aux espaces numériques de travail (ENT). En conséquence, il a la responsabilité de l'engagement de conformité au RU-003.

L'annuaire ENT permet directement ou à travers d'autres services d'offrir les fonctions suivantes :

- authentification des utilisateurs de l'ENT sur les applications de l'ENT et contrôle de leur accès à ces applications (notion « d'annuaire de sécurité ENT ») ;
- caractérisation et qualification des personnes ou des structures en relation avec l'ENT (notion « d'annuaire fonctionnel ENT »).

Dans la suite du document, seul le terme « annuaire ENT » sera utilisé.

En complément, l'annuaire ENT embarque des services de gestion des identités et d'administration des droits ou habilitations.

Ces services sont offerts exclusivement aux utilisateurs de l'ENT et aux applications reposant sur le socle ENT. Dans ce cas, les applications du socle ne gèreront pas en propre les données qui sont déjà disponibles dans l'annuaire ENT. Le document principal du SDET définit le contexte d'interopérabilité des ENT ; l'annexe opérationnelle du SDET précise les différentes nomenclatures de référence.

Des accès croisés sont attendus entre différents ENT. Il s'agit alors de permettre à un utilisateur d'un ENT d'accéder à des applications hébergées par un autre ENT.
Par ailleurs, l'ENT est au cœur d'un écosystème de plus en plus large, constitué par l'ensemble des entités et organisations qui interagissent dans un même environnement technologique (cf. chapitre 7 du document principal « Écosystème de l'ENT »).
Il est donc nécessaire de définir un cadre d'interopérabilité entre les ENT. Le document principal du SDET définit le contexte **d'interopérabilité** des ENT ; l'annexe opérationnelle du SDET précise les différentes nomenclatures de référence.

[1] Arrêté du 13 octobre 2017 modifiant l'arrêté du 30 novembre 2006 portant création, au sein du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche, d'un traitement de données à caractère personnel relatif aux espaces numériques de travail (ENT) (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000427578)

Conformément à l'arrêté du 30 novembre 2006 modifié par l'arrêté du 13 octobre 2017 relatif aux ENT, le système d'information (SI) du MEN constitue une source autoritaire majeure pour les données de l'annuaire ENT[2]. Des interfaces locales pourront si nécessaire être mises en place avec l'annuaire ENT. Enfin, l'annuaire ENT n'a pas, de son côté, vocation à alimenter les référentiels de différents SI à l'exception du Gestionnaire d'accès aux ressources (GAR) et des solutions de déploiement et de gestion des équipements informatiques ainsi que des outils de gestion de la classe conformes aux référentiels CARINE (cadre de référence des services d'infrastructures numériques d'établissements scolaires et d'écoles) et CARMO (cadre de référence pour l'accès aux ressources pédagogiques via un équipement mobile).

Pour l'enseignement agricole, le SI du ministère en charge de l'Agriculture est la source autoritaire majeure pour les données de l'annuaire ENT conformément à l'arrêté du 06/12/2007 relatif aux ENT[3]

2.2. Principes directeurs de l'annuaire ENT

Les principaux objectifs poursuivis à travers la définition du cahier des charges de l'annuaire ENT sont les suivants :

- **répondre à l'obligation légale** de lister les données à caractère personnel mentionnées dans l'article 4 de l'arrêté du 30 novembre 2006 modifié par l'arrêté du 13 octobre 2017
- **garantir l'interopérabilité** entre le SI du MEN et les ENT, mais également entre les ENT, le Gestionnaire d'accès aux ressources (GAR) et les services Tiers par la fourniture d'un standard commun ;
- **faciliter la construction des ENT** et garantir leur fonctionnement.

Ces objectifs sont à atteindre dans un environnement où les éléments contextuels suivants sont à prendre en compte :

Les projets ENT sont multiples, sur des périmètres différents. En conséquence, ils doivent généralement prendre en compte des ***spécificités*** *qui leur sont propres. Le cahier des charges n'a certainement pas été exhaustif dans la prise en compte de la* ***multiplicité des attentes****.*

Enfin, ces besoins multiples peuvent ***évoluer dans le temps****.*

L'approche suivante a alors été privilégiée :

- tous les besoins connus et conformes au cadre de l'annuaire ENT sont pris en compte en proposant un **modèle riche et des standards pour ce modèle** (*logique de faciliter la construction*) ;
- dans ce modèle, seul **un minimum**[4] **est obligatoire** et doit absolument respecter les standards proposés (*il s'agit d'un cadre à respecter pour garantir le fonctionnement de l'ENT, les accès inter-ENT, les accès au GAR et aux services Tiers*) *;*
- chaque ENT dispose **d'espaces de liberté propres** autour du minimum à respecter ; ces espaces de liberté concernent l'utilisation, l'ajout ou la suppression de certaines informations de l'annuaire (tant que le cadre d'interopérabilité est respecté) ou encore la mise en place de tel ou tel service (prise en compte des spécificités locales et de leurs évolutions dans le temps).

[2] Les modalités d'alimentation de l'annuaire ENT depuis le SI du MEN et d'autres SI externes sont détaillées à l'annexe 4.
[3] Arrêté du 6 décembre 2007 portant création au sein du ministère de l'Agriculture et de la Pêche d'un traitement de données à caractère personnel relatif aux espaces numériques de travail (ENT), publié au Journal officiel du 17 janvier 2008.
[4] Notons que le minimum est défini dans la suite du document par :
- Les identifiants pour les entrées utilisateurs, profils des utilisateurs et applications.
- Les attributs ou caractéristiques obligatoires dans l'annuaire ENT pour toutes les entrées (cf. chapitre 4.2).
- Les services de base de l'annuaire (cf. chapitre 6).

2.3. Vue d'ensemble de l'annuaire ENT

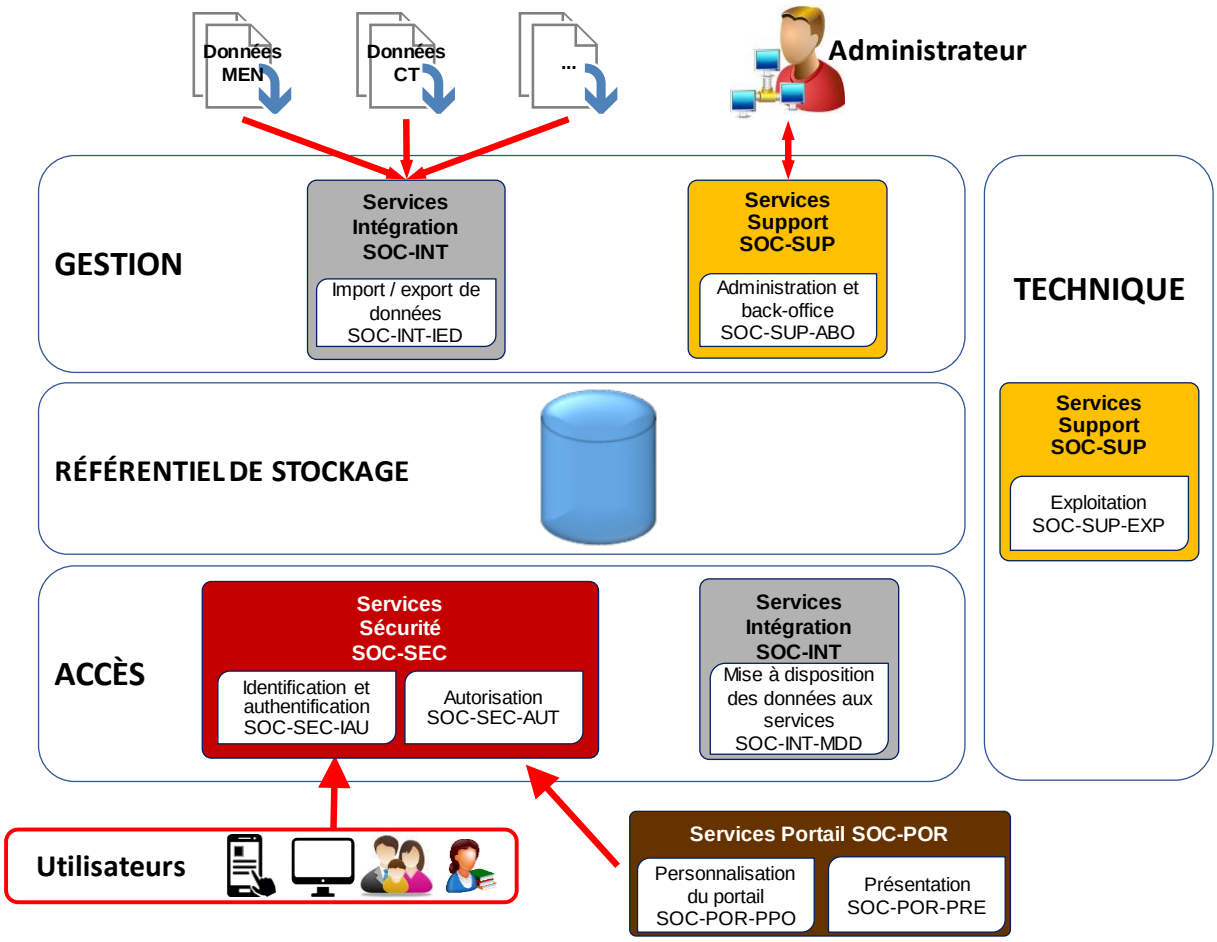

Figure 1 : Architecture fonctionnelle de la solution d'annuaire ENT pour le 2nd degré

Comme représenté en Figure 1, l'annuaire ENT ou la solution d'annuaire ENT se compose de plusieurs briques fonctionnelles :

- un **référentiel de stockage** contenant l'ensemble des données et des informations sur les personnes et les structures sur le périmètre couvert. Il propose plusieurs API (Application Programming Interface) d'accès à son contenu ;
- des **services de gestion** :
  - des fonctions d'alimentation, reposant sur le service Socle « Import / export de données », permettent de peupler et de mettre à jour l'annuaire ENT à partir de différentes sources de données, dont les extractions réalisées à partir à partir du SI du MEN et du SI du ministère en charge de l'Agriculture,
  - des fonctions de gestion des données annuaire, reposant sur le service Socle « Administration et back-office », permettent aux administrateurs et aux utilisateurs de modifier certaines informations contenues dans le référentiel ;
- des **services d'accès** :
  - des fonctions de sécurité reposant sur les services de sécurité « Identification et authentification » et « Autorisation » permettent de répondre aux requêtes d'authentification et d'autorisation,

  - des fonctions s'appuyant sur le service Socle « Mise à disposition des données aux services » permettent aux utilisateurs de visualiser le contenu de l'annuaire ENT ;
- des **services techniques** reposant sur le service Socle « Exploitation » permettent d'assurer la supervision, la gestion des traces et des audits, les sauvegardes et les restaurations.

Les attentes vis-à-vis de chacune de ces briques fonctionnelles sont détaillées dans la suite du document.

Notons que cette vue logique de l'annuaire ENT ne présume pas des orientations techniques qui doivent être proposées par le soumissionnaire. Le soumissionnaire précisera et justifiera dans sa réponse les orientations techniques qu'il a choisies.

3. Contenu de l'annuaire ENT

3.1. Périmètre des données

Le périmètre doit être adapté par le porteur en fonction des populations, des structures et des usages prévus par le projet ENT. Exemples : couverture des lycées uniquement, des Centres de formation des apprentis (CFA), des établissements agricoles…

Le périmètre couvert par l'annuaire ENT du projet [NOM_PROJET_ENT] regroupe l'ensemble des personnes et des structures liées à l'enseignement secondaire pour le périmètre suivant : À compléter par la maîtrise d'ouvrage en charge du projet ENT : départements et régions concernés.

3.1.1. Catégories de personnes

Rapportés au périmètre du projet ENT, les catégories de personnes concernées par l'annuaire ENT sont les suivantes :

- les **élèves scolarisés dans un établissement du second degré** ;
- les **personnes en relation avec les élèves scolarisés dans un établissement du second degré** (couvre les personnes exerçant l'autorité parentale, les personnes hébergeant un élève, les responsables financiers, les correspondants en cas d'urgence) ;
- les **enseignants exerçant une activité au sein du projet** (qu'ils soient rattachés à un établissement du second degré ou à des services académiques) ;
- les **non enseignants rattachés administrativement à un établissement du second degré** (couvre les chefs d'établissement, les responsables d'enseignement spécialisé, certains personnels administratifs ainsi que les personnels des établissements privés) ;
- les **non enseignants rattachés administrativement à des services académiques** et exerçant une activité au sein du projet (couvre les corps d'inspection et les personnels détachés du rectorat) ;
- les **non enseignants rattachés administrativement à une collectivité locale** et exerçant une activité au sein du projet (couvre les techniciens et ouvriers de service) ;
- les **personnes extérieures intervenant pour un établissement** du second degré (couvre les personnels sociaux et de santé, le personnel d'orientation, les syndicats et associations de parents d'élèves siégeant en conseil d'administration, les prestataires, les invités) ;
- les **tuteurs de stage et maîtres d'apprentissage** des élèves ;
- les **responsables des entreprises, associations ou entités partenaires** des établissements d'enseignement secondaire et des services académiques.

3.1.2. Catégories de structures

Les structures concernées par l'annuaire ENT du projet sont les suivantes :

- les **établissements d'enseignement** secondaire appartenant au périmètre du projet. Il peut s'agir de tout ou partie des structures d'enseignement référencées par le MEN ou le ministère en charge de l'Agriculture et disposant à ce titre d'un numéro UAI (ex-RNE)
(couvre a minima les collèges et les lycées, qu'ils soient publics ou privés, les établissements d'enseignement agricole) ;

- les **autorités et services académiques** appartenant au périmètre du projet.
  (couvre a minima le rectorat ou vice-rectorat, les directions académiques des services départementaux de l'Éducation nationale (DSDEN) les services des DSDEN et pour l'enseignement agricole la direction régionale de l'Alimentation, de l'Agriculture et de la Forêt (DRAAF-DAF) et les services régionaux de la Formation et du Développement (SFRD)) ;
- les **collectivités locales** appartenant au périmètre du projet
  (couvre a minima les conseils régionaux et les conseils départementaux) ;
- les **entreprises partenaires** des établissements d'enseignement secondaire et des services académiques appartenant au périmètre du projet
  (couvre a minima les entreprises accueillant des élèves de l'académie en stage ou en apprentissage, les entreprises formant des apprentis, les Chambres de Commerce et d'Industrie et les partenaires socio-culturels).

3.2. Modèle de sécurité

Le modèle de sécurité de l'annuaire ENT décrit les associations entre les personnes, les profils applicatifs, les rôles applicatifs et les applications afin de définir les niveaux d'habilitations des acteurs de l'ENT aux différentes applications qui leur sont proposées.

Le soumissionnaire pourra cependant proposer et justifier une solution technique alternative pour gérer les habilitations au sein de sa solution et non au sein de l'annuaire ENT. Il devra alors décrire l'ensemble des modifications à apporter, notamment au modèle et à l'architecture technique.

Ce modèle de sécurité de l'annuaire ENT est représenté en Figure 2.

Chaque élément est décrit dans la suite du chapitre.

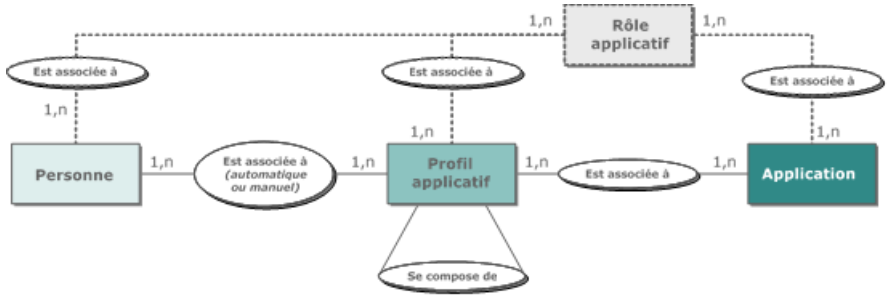

Figure 2 : Modèle de sécurité de l'annuaire ENT

3.2.1. « Personne »

Une Personne est un membre d'une des catégories de personnes définies sur le périmètre adressé par l'annuaire ENT.

Une Personne peut être associée à plusieurs Profils applicatifs.

Une Personne peut être directement associée (si nécessaire) à plusieurs Rôles applicatifs.

3.2.2. « Profil applicatif »

Un Profil applicatif est un objet de sécurité permettant le regroupement de Personnes selon des caractéristiques particulières propres à la Personne afin de faciliter les actes d'administration.

Le Profil applicatif peut être défini par rapport à différents niveaux :

- « niveau projet » : identique pour tous les établissements du projet, il permet à un individu d'avoir un profil applicatif permettant des accès aux mêmes services quel que soit l'établissement interne au projet ;
- « niveau établissement » : il permet de personnaliser un profil applicatif particulier à l'établissement.

Un Profil applicatif peut être peuplé selon trois modes :

- « mode Automatique »[5] : une règle de peuplement détermine dynamiquement les Personnes qui appartiennent à un Profil applicatif. Seuls les attributs marqués par une croix dans la colonne « Autorisa. » du tableau de l'annexe 2 peuvent être utilisés pour définir des règles de peuplement.
  Exemple de règle de peuplement d'un profil correspondant aux élèves de Première et de Terminale technologiques : (classe d'objet = « Élève ») ET (filière = « Technologique ») ET ((niveau = « Première ») OU (niveau = « Terminale »))
- « mode Discrétionnaire » : les gestionnaires affectent manuellement des Personnes à un Profil applicatif.
- « mode Mixte » : les deux modes précédents sont utilisés pour peupler le Profil applicatif.

La maîtrise d'ouvrage en charge du projet ENT pourra, si elle le souhaite, baser les règles de peuplement sur des attributs supplémentaires et donc modifier en fonction la liste donnée en annexe 2.
La réplication filtrée (cf. chapitre 5.1) devra être adaptée en conséquence.

Les Profils applicatifs peuvent également être imbriqués (un Profil applicatif peut regrouper d'autres Profils applicatifs) ou exclusifs (cf. chapitre 6.1.2).

La liste des Profils applicatifs d'une Personne peut également être utilisée dans la règle de peuplement.
Exemple de règle de peuplement d'un profil applicatif regroupant l'ensemble du personnel administratif : (profil = « Secrétariat ») ET (profil = « Personnel de direction »)

3.2.3. « Application »

Une Application désigne tout service applicatif proposé aux Personnes et utilisant les services du socle ENT.

Les Applications utilisent tout d'abord les services Sécurité [SOC-SEC][6] pour contrôler l'authentification d'une Personne en vérifiant la validité des identifiants et des moyens d'authentification présentés.

Les Applications utilisent ensuite les services Sécurité [SOC-SEC] pour contrôler l'accès de la Personne à l'Application. Les services Sécurité [SOC-SEC] permettent de vérifier :

- la valeur de certains attributs de la Personne (les applications peuvent baser leurs autorisations sur certains attributs du modèle. Ces attributs sont marqués par une croix dans la colonne « Autorisa. » de l'annexe 2.)
- et/ou l'appartenance de la Personne à au moins un des Profils applicatifs liés à l'Application.

L'Application utilise les Profils applicatifs pour définir des droits d'accès macroscopiques.

[5] Une règle de peuplement automatique d'un Profil applicatif correspond à une expression logique sur des couples « attribut / valeur ». Toute Personne dont les attributs vérifient l'expression logique est automatiquement affectée au Profil applicatif.
[6] Trigramme utilisé dans l'architecture de référence des ENT décrite dans le document principal du SDET

La maîtrise d'ouvrage en charge du projet ENT pourra, si elle le souhaite, baser les autorisations sur des attributs supplémentaires et donc modifier en fonction la liste donnée en annexe 2.
La réplication filtrée (cf. chapitre 5.1) devra être adaptée en conséquence.

3.2.4. « Rôle applicatif »

Une Application peut également définir des Rôles applicatifs dans l'annuaire ENT. Un Rôle applicatif donne accès à un ensemble de fonctionnalités au sein de l'application pour laquelle a été défini le Rôle applicatif.

Un Rôle applicatif est défini pour une ou plusieurs Applications. Un Rôle applicatif peut être associé à plusieurs Profils applicatifs et plusieurs Personnes directement.

La gestion de droits plus fins reste du ressort des Applications.

3.2.5. Exemple

La maîtrise d'ouvrage en charge du projet ENT pourra, si elle le souhaite, supprimer ou adapter cet exemple.

Une application de gestion du budget de l'établissement déclare dans l'annuaire ENT des rôles applicatifs, qui pour l'application ont la signification suivante :

- *« Responsable » : a accès à toutes les fonctions de l'application ;*
- *« Gestionnaire » : a accès aux fonctions de visualisation et de modification ;*
- *« Utilisateur » : a accès à la fonction de visualisation.*

Les profils applicatifs « Personnels de direction » et « Personnels d'intendance » sont associés au rôle « Responsable », le profil applicatif « Personnels administratifs » est associé au rôle « Gestionnaire » et le profil applicatif « Conseillers d'éducation » est associé au rôle « Utilisateur ». Le rôle applicatif « Responsable » est directement attribué à une des personnes.

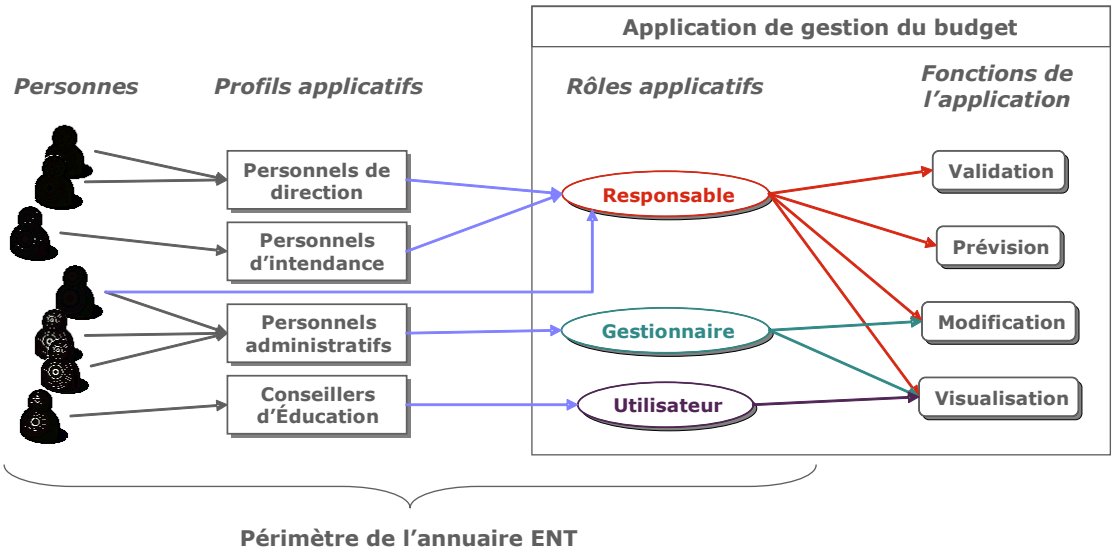

Figure 3 : Exemple de gestion des droits sur une application de l'ENT

3.2.6. Remarques

Le présent document est basé sur les spécifications du socle ENT et des fonctions standard attendues des services Sécurité [SOC-SEC]. À ce stade, il ne tient pas compte de fonctionnalités spécifiques portées par les services Sécurité [SOC-SEC] proposés par le soumissionnaire, par exemple challenges, prise en compte de la période d'accès dans l'autorisation, de la typologie d'accès, fonction de suspension d'utilisateurs après échecs…

Le soumissionnaire précisera les impacts de ces fonctions sur le modèle de données de l'annuaire.

Le modèle présenté peut éventuellement être adapté ou limité en fonction des implémentations proposées par le soumissionnaire :

- Exemples de limitations : pas d'utilisation des groupes dynamiques, limitation de la taille des groupes statiques…
- Exemples d'adaptations : utilisation de la classe d'objet ou d'une combinaison d'attributs existants pour déterminer l'appartenance à un profil applicatif partagé… Des solutions différentes pourront notamment être proposées en fonction des catégories de personnes, du fait des différences de volumétrie et de la possibilité ou non d'utiliser la classe d'objet pour déterminer l'appartenance à un profil.

Le soumissionnaire précisera donc, en fonction des capacités des services AAS qu'il propose et de l'impact de la volumétrie sur les performances (cf. chapitre 7), les limitations et les adaptations proposées sur le modèle de sécurité.

Le soumissionnaire pourra également adapter le modèle afin de définir des habilitations à partir des groupes de personnes. Il devra alors décrire l'ensemble des modifications à apporter à ce modèle de sécurité.

3.3. Caractérisation des personnes

Ce chapitre définit les catégories de personnes et de structures de l'annuaire ENT qui ont été présentées au chapitre 3.1.

Le modèle ci-après prend en compte le fait qu'une personne puisse appartenir à plusieurs catégories. Il peut s'agir par exemple d'un enseignant qui est également parent d'un élève ou encore d'un enseignant qui assure des fonctions administratives dans un établissement (chef d'établissement notamment).

La figure suivante est une illustration de la caractérisation des personnes de l'annuaire ENT.

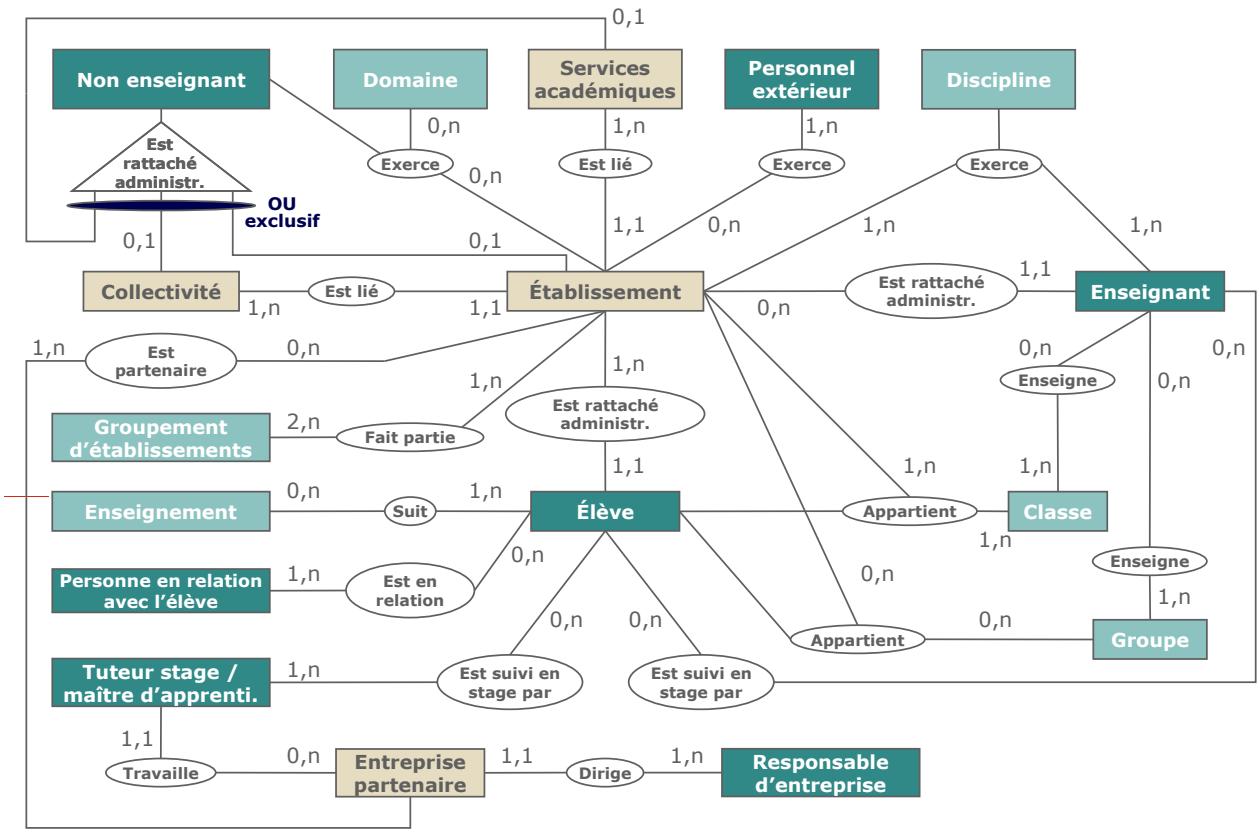

Figure 4 : Caractérisation des personnes de l'annuaire ENT

Les paragraphes ci-après expliquent les relations entre les différents éléments du modèle.

Une description détaillée de chaque élément du modèle d'information est donnée à l'annexe 2.

3.3.1. Description des personnes

3.3.1.1. Élève

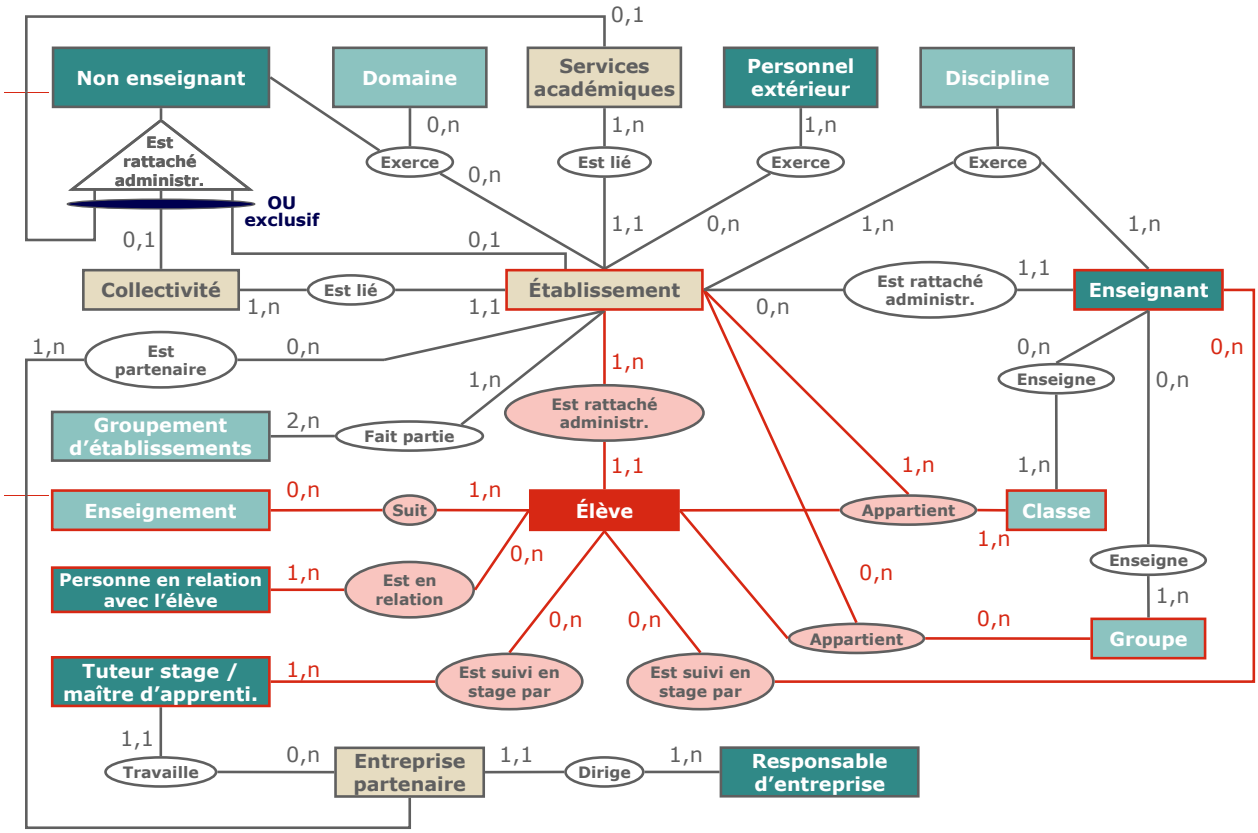

Figure 5 : Caractérisation d'un Élève

Un *Élève* est rattaché administrativement à un et un seul *Établissement*.

Un *Élève* est en relation avec zéro (élève majeur), une, ou plusieurs *Personnes en relation avec l'élève*.

Un *Élève* suit un ou plusieurs *Enseignements*.

Un *Élève* effectue zéro ou un stage/apprentissage simultanément. Pour ce stage/apprentissage, il est suivi par un ou plusieurs *Enseignants*, et un ou plusieurs *Tuteurs de stage ou maîtres d'apprentissage*. **Parmi les *Enseignants* qui suivent l'*Élève* durant son stage/apprentissage, un seul est responsable de l'*Élève*.**

Un *Élève* appartient à zéro, un, ou plusieurs *Groupes*. Ces *Groupes* peuvent se trouver dans des *Établissements* différents.

Un *Élève* appartient au moins à une *Classe*. Un *Élève* peut appartenir à plusieurs *Classes*, **mais à une seule *Classe* par *Établissement***.

Remarque : Dans certains cas, un élève peut être amené à utiliser plusieurs ENT. En effet, si un élève suit des enseignements dans un établissement autre que son établissement de rattachement administratif et que les deux établissements ne sont pas « couverts » par le même ENT, cet élève est géré dans les deux ENT. Ce besoin d'accès à de multiples ENT peut également concerner des enseignants, des personnes en relation avec l'élève ou des non enseignants.

3.3.1.2. Personne en relation avec l'élève

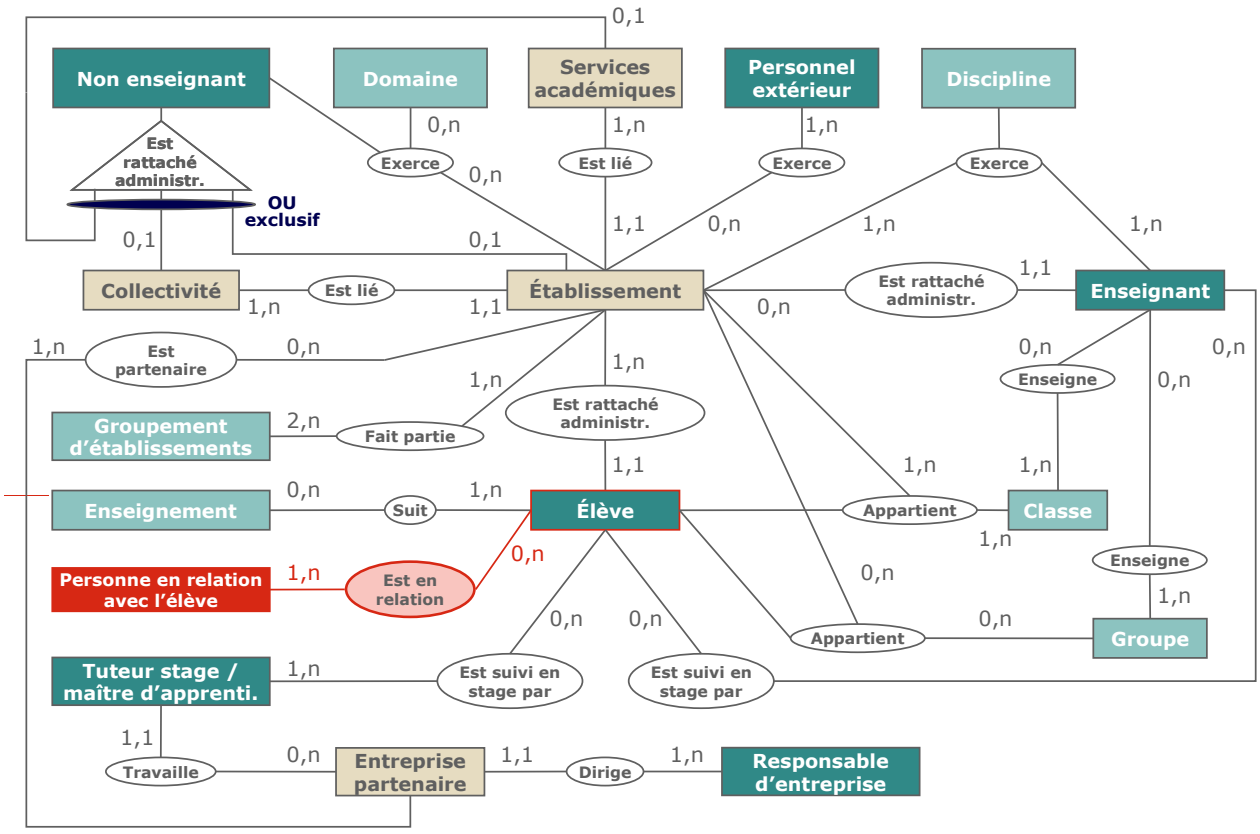

Figure 6 : Caractérisation d'une Personnes en relation avec un élève

Une *Personne en relation avec l'élève* est en relation avec un ou plusieurs *Élèves*.

3.3.1.3. Enseignant

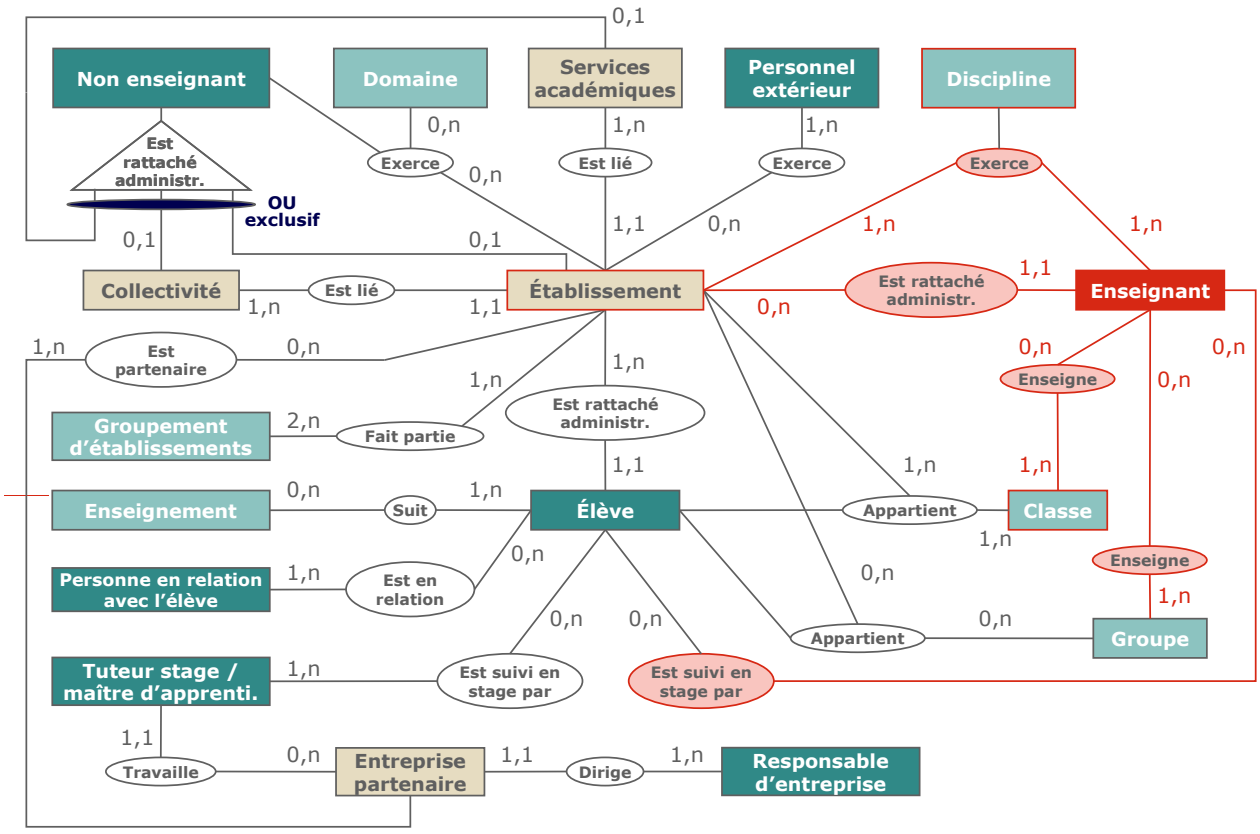

Figure 7 : Caractérisation d'un Enseignant

Un *Enseignant* est rattaché administrativement à un et un seul *Établissement*.

Un *Enseignant* exerce une ou plusieurs *Disciplines* dans un ou plusieurs *Établissements*.

Un *Enseignant* enseigne dans zéro, une, ou plusieurs *Classes*.

Un *Enseignant* enseigne dans zéro, un, ou plusieurs *Groupes*.

Un *Enseignant* suit zéro, un, ou plusieurs *Élèves* durant leur stage/apprentissage. **Parmi les *Enseignants* qui suivent un *Élève* durant son stage/apprentissage, un seul est responsable de l'*Élève*.**

3.3.1.4. Non enseignant

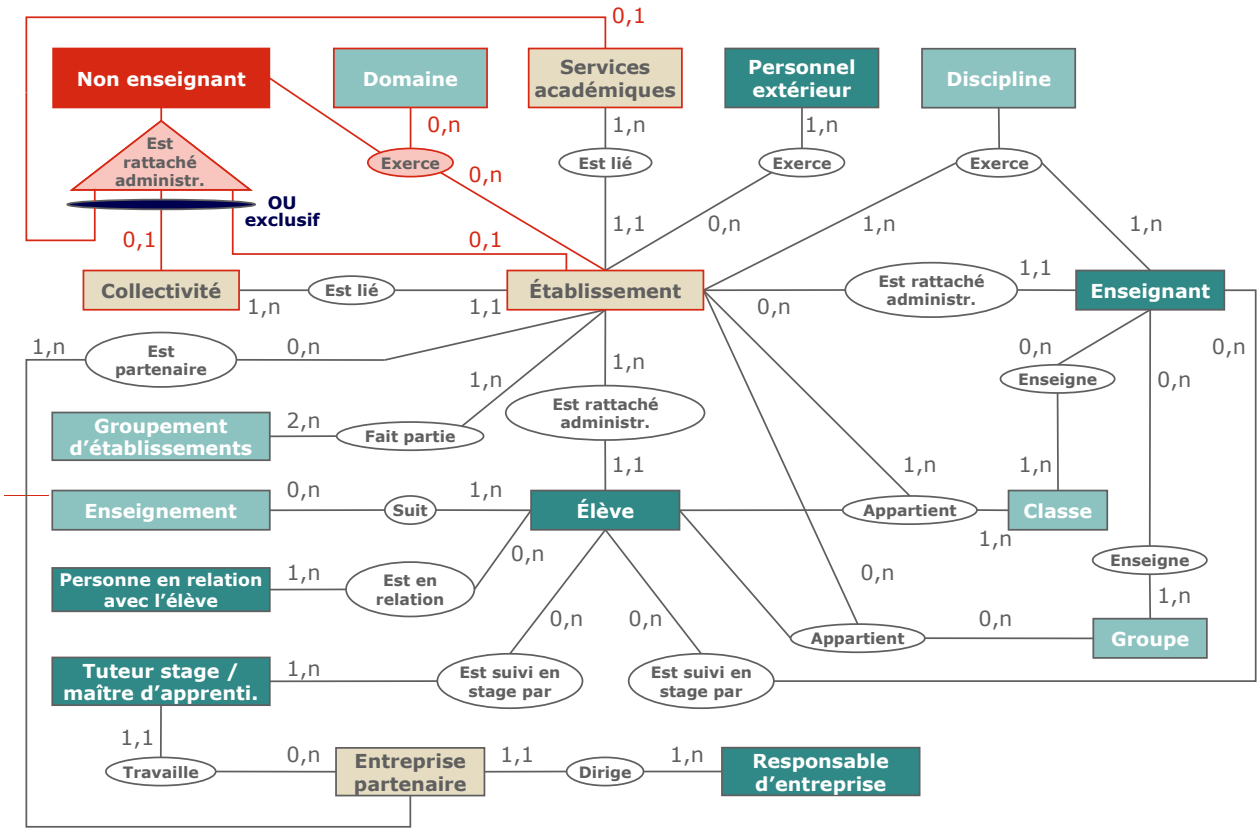

Figure 8 : Caractérisation d'un Non enseignant

Un *Non enseignant* peut exercer une activité dans un ou plusieurs *Domaines*, dans un ou plusieurs *Établissements*.

Un *Non enseignant* est lié soit à une et une seule *Collectivité locale*, soit à un et un seul ensemble de *Services académiques*, soit à un et un seul *Établissement*.

3.3.1.5. Personnel extérieur

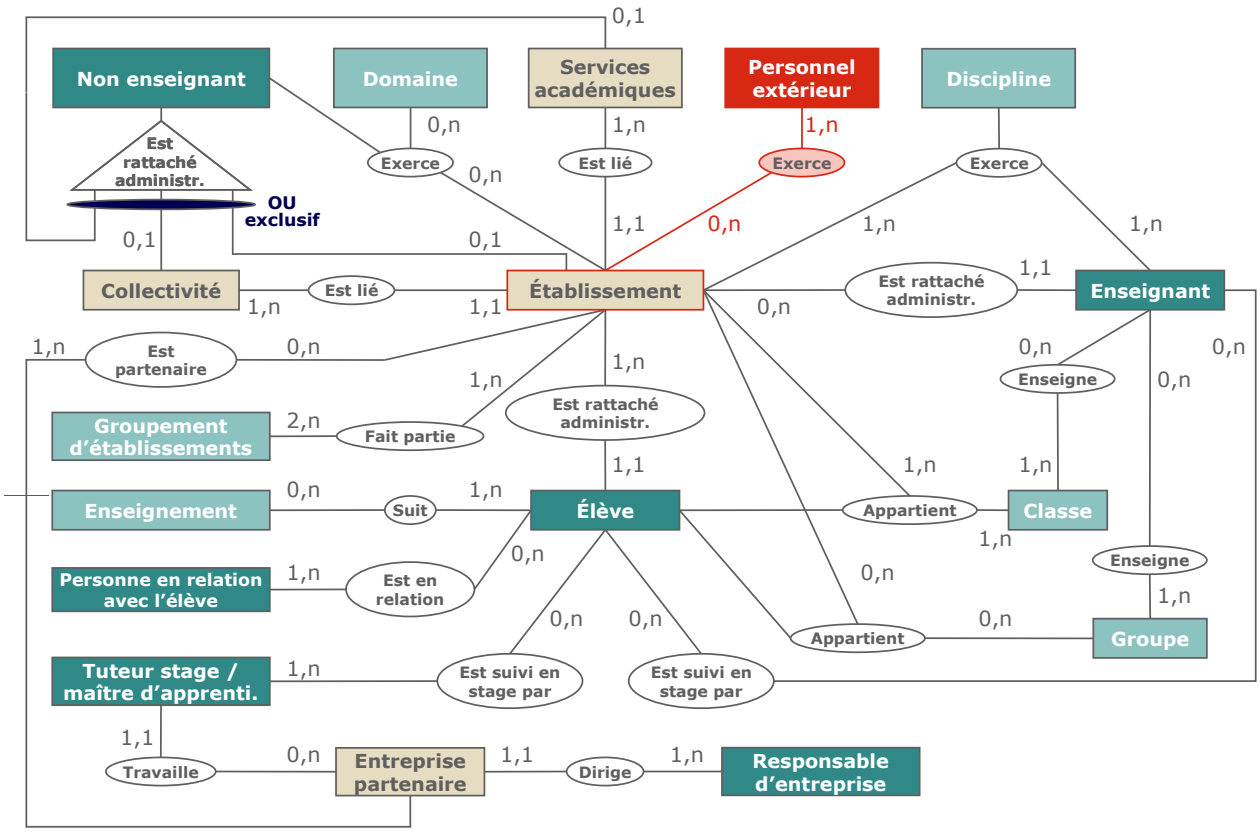

Figure 9 : Caractérisation d'un Personnel extérieur

Un *Personnel extérieur* exerce une activité dans un ou plusieurs *Établissements*.

3.3.1.6. Tuteur de stage ou maître d'apprentissage

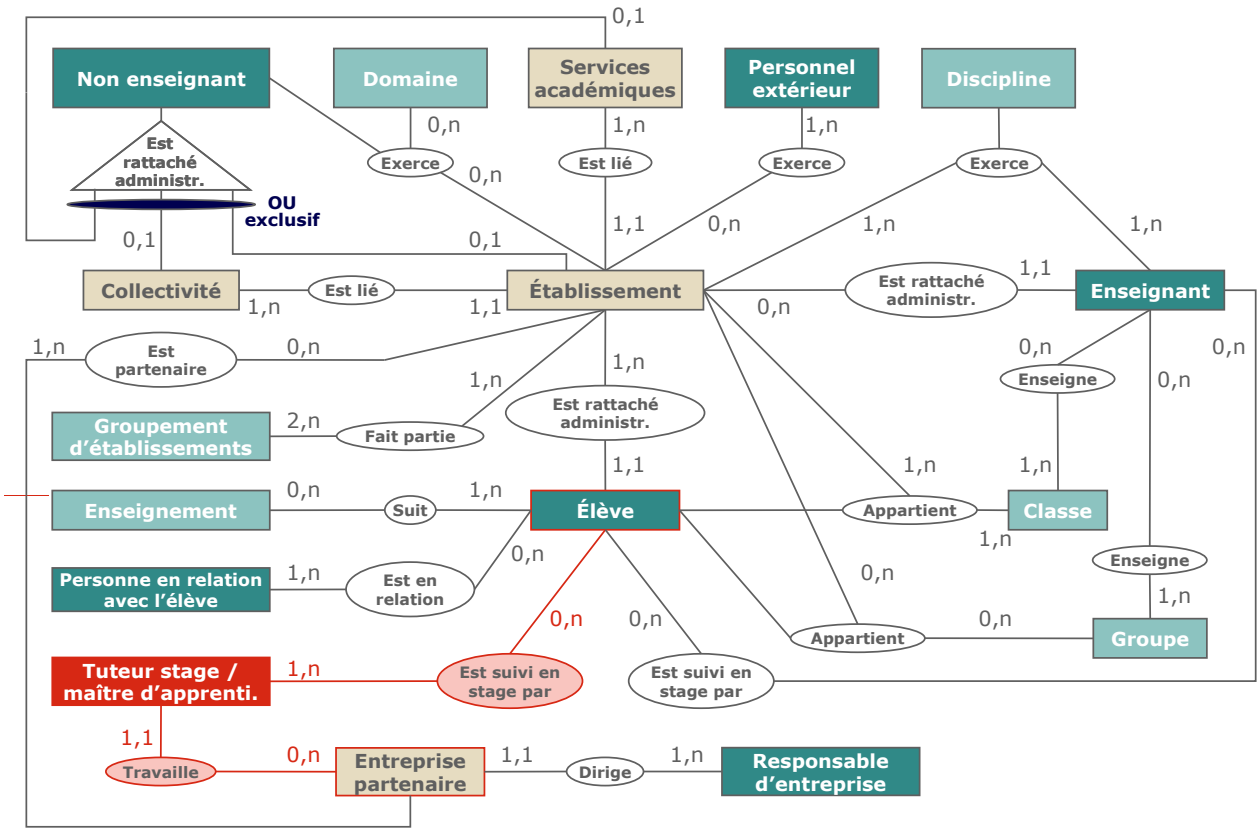

Figure 10 : Caractérisation d'un Tuteur de stage ou maître d'apprentissage

Un *Tuteur de stage ou maître d'apprentissage* suit un ou plusieurs *Élèves* durant leur stage/apprentissage.

Un *Tuteur de stage ou maître d'apprentissage* travaille dans une *Entreprise partenaire*.

3.3.1.7. Responsable d'entreprise

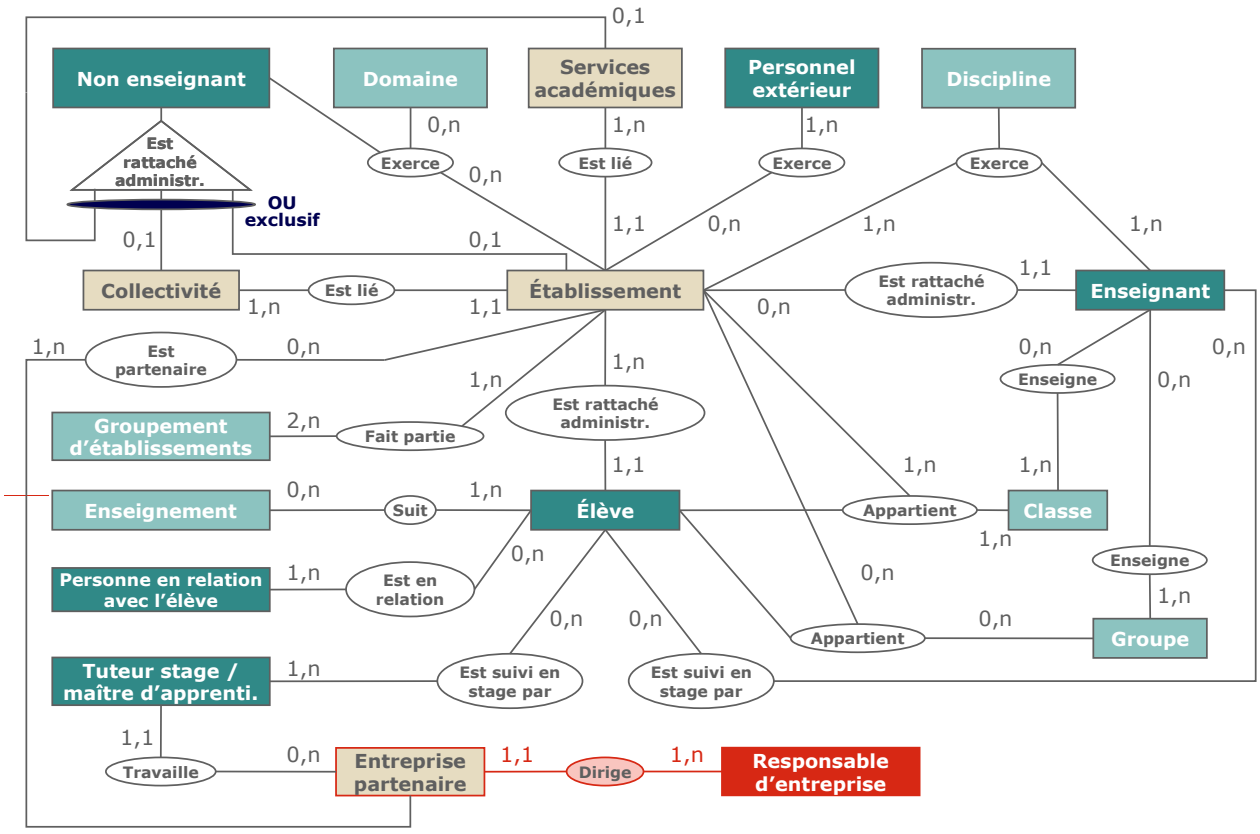

Figure 11 : Caractérisation d'un Responsable d'entreprise

Un Responsable d'entreprise est responsable d'une ou plusieurs Entreprises partenaires.

3.3.2. Description des structures liées aux personnes

3.3.2.1. Établissement

À un *Établissement* sont rattachés administrativement un ou plusieurs *Élèves*.

Un *Établissement* est lié à une et une seule *Collectivité locale*.

Un *Établissement* est lié à un et un seul ensemble de *Services académiques*.

À un *Établissement* sont rattachés administrativement zéro, un, ou plusieurs *Non enseignants*.

Dans un *Établissement*, zéro, un, ou plusieurs *Non enseignants* (rattachés administrativement ou non) peuvent exercer une activité dans un ou plusieurs *Domaines*.

Dans un *Établissement*, zéro, un, ou plusieurs *Personnels extérieurs* peuvent exercer une activité.

Dans un *Établissement* sont exercées une ou plusieurs *Disciplines* par un ou plusieurs *Enseignants*.

Un *Établissement* possède une ou plusieurs *Classes*.

Un *Établissement* possède zéro, un, ou plusieurs *Groupes*.

Un *Établissement* fait partie de zéro, un, ou plusieurs *Groupements d'établissements*.

Un *Établissement* est partenaire d'une ou plusieurs *Entreprises partenaires*.

3.3.2.2. Collectivité locale

Une *Collectivité locale* est liée à un ou plusieurs *Établissements*.

À une *Collectivité locale* sont rattachés administrativement zéro, un ou plusieurs *Non enseignants*.

3.3.2.3. Services académiques

Un ensemble de *Services académiques* est liée à un ou plusieurs *Établissements*.

À un ensemble de *Services académiques* sont rattachés administrativement zéro, un ou plusieurs *Non enseignants*.

3.3.2.4. Entreprise partenaire

Une Entreprise partenaire est dirigée par un et un seul Responsable d'entreprise.

Une Entreprise partenaire est partenaire d'un ou plusieurs Établissements.

Dans une Entreprise partenaire travaillent zéro, un ou plusieurs Tuteurs de stage ou maîtres d'apprentissage.

3.3.3. Description des autres types de données liés aux personnes

3.3.3.1. Domaine

Un *Domaine* peut correspondre à l'activité d'un ou plusieurs *Non enseignants* dans un ou plusieurs *Établissements*.

3.3.3.2. Discipline

Une *Discipline* peut être exercée par un ou plusieurs *Enseignants* dans un ou plusieurs *Établissements*.

3.3.3.3. Classe

Une *Classe* appartient à un et un seul *Établissement*.

Une *Classe* regroupe un ou plusieurs *Élèves* qui peuvent être rattachés administrativement à des *Établissements* différents.

Une *Classe* reçoit l'*Enseignement* d'un ou plusieurs *Enseignants*.

3.3.3.4. Groupe

Un *Groupe* appartient à un et un seul *Établissement*.

Un *Groupe* regroupe zéro, un, ou plusieurs *Élèves* qui peuvent être rattachés administrativement à des *Établissements* différents.

Un *Groupe* reçoit l'*Enseignement* d'un ou plusieurs *Enseignants*.

3.3.3.5. Groupe libre (créé dans un établissement) ou groupe Adhoc

Un *Groupe* Adhoc appartient à un et un seul établissement

Un groupe Adhoc peut contenir des personnes de plusieurs établissements

Un Groupe Adhoc regroupe zéro, une, ou plusieurs personnes

Un Groupe Adhoc n'a plus lieu d'être s'il est vide

3.3.3.6. Enseignement

Un *Enseignement* est suivi par zéro, un, ou plusieurs *Élèves*.

3.3.3.7. Groupement d'établissements

Un *Groupement d'établissements* regroupe deux ou plus *Établissements*. Le terme *Groupement d'établissements* inclut les bassins de formation, les cités scolaires et les GRETA.

3.3.4. Contraintes d'intégrité

Des contraintes d'intégrité sur les données de l'annuaire ENT viennent compléter la description présentée ci-dessus. Ces contraintes sont les suivantes :

[CI-1] Au plus trois[7] *Personnes en relation avec l'élève* exercent l'autorité parentale sur cet *Élève*.

[CI-2] Au moins une *Personne en relation avec l'élève* exerce l'autorité parentale sur un *Élève* mineur.

[CI-3] Sur décision d'un *Élève* majeur, il est possible qu'aucune *Personne en relation avec l'élève* n'exerce l'autorité parentale sur lui.

[CI-4] Il existe au plus deux[8] professeurs principaux par *Classe*.

[CI-5] Un professeur principal d'une classe donnée enseigne nécessairement au moins une discipline à cette *Classe* ou à un *Groupe* appartenant à cette *Classe*.

[CI-6] Il existe au plus deux *Élèves* délégués par *Classe*.

[CI-7] Un *Élève* délégué de classe doit nécessairement faire partie de la *Classe* dont il est le délégué.

[7] Conformément à la loi n°2002-305 du 4 mars 2002

[8] Conformément au décret n° 2017-1637 du 30 novembre 2017 modifiant le décret n° 93-55 du 15 janvier 1993 instituant une indemnité de suivi et d'orientation des élèves en faveur des personnels enseignants du second degré (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036121232)

[CI-8] Le contact ENT par défaut d'un établissement est le chef d'établissement de cet établissement.

[CI-9] Un Mef de rattachement est un Mef national. Le dernier caractère doit donc être « 0 ».

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement compléter cette liste si d'autres contraintes d'intégrité doivent être prises en compte.

4. Schéma et DIT de l'annuaire ENT

4.1. Préambule

4.1.1. Orientation technologique

L'annuaire ENT doit répondre à des requêtes correspondant à différents usages :

- des requêtes d'authentification / autorisation ;
- des requêtes de consultation ;
- des requêtes de mise à jour / gestion.

L'annuaire ENT s'appuie sur plusieurs référentiels typés par usage (cf. chapitre 5) :

- un référentiel pour les mises à jour, la gestion et la consultation d'informations ;
- un référentiel pour l'authentification et l'autorisation des utilisateurs.

Tous ces référentiels sont des annuaires compatibles LDAP v3.

Quelques éléments ayant guidé ce choix :

- LDAP est utilisé en standard pour des référentiels de sécurité (devant offrir des services d'authentification / autorisation).
- Le choix de LDAP pour l'ensemble des référentiels typés par usage permet d'assurer une cohérence technologique entre les différents référentiels et de faciliter la mise en œuvre des flux de synchronisation.

Le soumissionnaire pourra cependant proposer et justifier une solution technique alternative pour les référentiels. Il devra alors décrire l'ensemble des modifications à apporter, notamment au modèle et à l'architecture technique.

Dans tous les cas, l'annuaire ENT doit pouvoir être exporté dans un format ouvert et documenté tel que LDIF ou DSML.

4.1.2. Organisation des OID de l'annuaire ENT

Ce chapitre est à compléter par le porteur.

Cas n°1 : Si la maîtrise d'ouvrage en charge du projet ENT possède ou souhaite posséder un OID propre pour son organisation[9], celui-ci sera utilisé comme arc principal pour l'identification des éléments du schéma LDAP.

[9] Une demande d'OID peut être effectuée auprès de l'IANA ou de l'AFNOR.

La règle de hiérarchisation est la suivante :
<OID porteur>.<projet>.<type usage>.<portée>.<type d'élément>.<incrément>
avec :
<OID porteur> : OID attribué à la maîtrise d'ouvrage en charge du projet ENT, soit « À COMPLETER »
<projet> : vaut « 1 » pour le projet ENT
<usage> : vaut « 1 » pour l'annuaire ENT
<portée> : définit s'il s'agit d'un objet commun aux ENT ou d'une extension locale (« 1 » : objet du modèle commun à tous les ENT, « 2 » : extension locale de schéma)
<type d'élément> : définit le type d'élément identifié (« 1 » : attribut, « 2 » : classe d'objet)
<incrément> : nombre à incrémenter pour chaque objet créé

Les valeurs de <incrément> à utiliser pour les classes et les attributs du modèle de l'annuaire ENT sont données en annexe 3.

Cas n°2 : sinon, la maîtrise d'ouvrage en charge du projet ENT utilisera l'OID de son choix et utilisera la règle de hiérarchisation présentée ci-dessus.

4.1.3. Nomenclatures

Les nomenclatures correspondant aux attributs du schéma LDAP sont données en annexe 3.

La maîtrise d'ouvrage en charge du projet ENT devra préciser les nomenclatures qu'elle souhaite partager au niveau de tout l'ENT. Dans le cas contraire, hors nomenclature à portée nationale, la nomenclature sera propre à un établissement et non partagée dans l'ENT.

4.2. Description des classes d'objet de l'annuaire ENT

Remarques :

- Des précisions sur les notions liées à la scolarité (MEF, matières, UAI…) sont données dans l'annexe opérationnelle du SDET.
- Sauf mention contraire, les « classes » dont il est question dans ce chapitre sont des classes au sens LDAP.

4.2.1. Gestion des objets de l'annuaire ENT

4.2.1.1. Personnes appartenant à plusieurs catégories de personnes

Une personne peut appartenir à plusieurs catégories de personnes. Il peut s'agir par exemple d'un enseignant qui est également parent d'un élève.

L'entrée de l'annuaire ENT représentant une telle personne doit disposer de l'ensemble des caractéristiques propres à chacune des catégories de la personne.

C'est pourquoi le schéma de l'annuaire ENT est basé sur l'utilisation de **classes LDAP auxiliaires**, qui permettent de compléter une entrée de l'annuaire ENT avec des attributs spécifiques. En cumulant plusieurs classes auxiliaires sur l'entrée d'une même personne, celle-ci disposera de tous les attributs nécessaires en fonction des catégories de personnes auxquelles elle appartient.

Exemple de création d'un enseignant qui est également parent d'un élève :

- *Un objet est créé à partir de la classe ENTPerson. L'objet dispose ainsi des attributs communs à tous les utilisateurs de l'ENT.*
- *La personne étant enseignante, il faut ajouter la classe auxiliaire ENTAuxEnseignant à l'objet. Celui-ci dispose alors d'attributs tels que les disciplines enseignées, les classes dont la personne est professeur principal…*
- *Étant également parent, il faut ajouter la classe auxiliaire ENTAuxPersRelEleve à l'objet. Celui-ci dispose alors d'attributs tels que les élèves en responsabilité…*

Il n'est pas possible de restreindre les classes LDAP structurelles que peut venir compléter une classe auxiliaire. Un contrôle d'intégrité devra donc être assuré au niveau des services de gestion de contenu afin de ne permettre l'ajout de classes auxiliaires qu'à la classe structurelle *ENTPerson*. Les élèves (classe *ENTEleve*) ne peuvent en effet pas appartenir à plusieurs catégories.

Par ailleurs, l'ENT pourra offrir aux utilisateurs un service permettant de réconcilier les identités distinctes qu'ils possèdent dans chacune des catégories (cf. [SRV-3] au chapitre 6.1.1).

4.2.1.2. Personnes exerçant dans plusieurs établissements

Certaines personnes exercent leur activité dans plusieurs établissements : des élèves suivent des cours dans plusieurs établissements, des personnels administratifs dépendant d'une collectivité locale possèdent des fonctions dans un établissement d'enseignement…

En conséquence, ces personnes accèdent à plusieurs ENT d'établissement. Selon les cas, ces ENT relèvent du même projet ENT ou de projets différents (les possibilités de rapprochement des comptes sont donc différentes).

Il est donc nécessaire de distinguer la structure de rattachement administratif et la ou les structures d'exercice. C'est pourquoi tout utilisateur de l'ENT possède l'attribut « ENTPersonStructRattach » pour désigner la structure de rattachement administratif. Les structures d'exercice doivent par contre être déduites de l'attribut « ENTPersonFonctions ».

4.2.1.3. Qualification des relations multiples entre objets de l'annuaire ENT

Une certaine complexité peut apparaître dans le schéma LDAP lorsqu'il est nécessaire de qualifier des relations « n – n » entre objets.
Exemple : « Comment qualifier la relation entre un élève et une personne, sachant qu'un élève peut être en relation avec plusieurs personnes dont le rôle est différent, et qu'une personne peut être en relation avec plusieurs élèves et jouer un rôle différent vis-à-vis de chaque élève ? ».

Afin de qualifier d'éventuelles relations supplémentaires concernant un *Élève*, il est possible d'utiliser la classe *ENTRelEleve*. Une instance de ce groupe doit être créée pour chaque relation entre chaque couple « *Élève – Personne en relation avec l'élève* ». Un attribut du groupe permet de qualifier cette relation. Il conviendra toutefois d'être attentif au volume d'entrées supplémentaires générées dans l'annuaire ENT par cette solution.

Afin de transmettre les informations issues de SIECLE (ex-SCONET), l'attribut ENTElevePersRelEleve contient le dn de la personne en relation suivi des « codes » type de relation, responsable financier, responsable légal, contact, beneficiaire.
Remarque : Ces informations sont cependant amenées à évoluer du fait de l'évolution de la gestion des responsables dans SIECLE.

4.2.1.4. Adultes en formation continue

Les adultes en formation continue ne sont pas pris en compte dans le schéma proposé. Si la maîtrise d'ouvrage en charge du projet ENT souhaite les intégrer au périmètre couvert par l'ENT, elle devra ajouter une classe auxiliaire « ENTAuxFormationContinue », déterminer les attributs nécessaires pour cette classe et assurer l'alimentation de cette nouvelle catégorie de personnes.

4.2.2. Schéma LDAP

Les classes LDAP standard sont utilisées autant que possible afin de faciliter la mise en place d'applications génériques. Les attributs non disponibles dans le schéma standard sont ajoutés dans des classes dédiées à l'ENT par extension du schéma.

Le schéma LDAP de l'annuaire ENT est représenté sur la Figure 12. Les différentes classes sont décrites dans la suite du chapitre et sont reprises à **l'annexe 3**.

Le récapitulatif des attributs par catégorie de personnes ou de structures est donné à **l'annexe 2**. Notons que le caractère facultatif ou obligatoire d'un attribut hérité peut varier en fonction de la catégorie de personnes ou de structures.

Remarque : Des attributs à caractère technique pourront être ajoutés au schéma LDAP afin de couvrir les besoins des services Sécurité [SOC-SEC] (utilisateur suspendu, date de validité, « challenges »…).

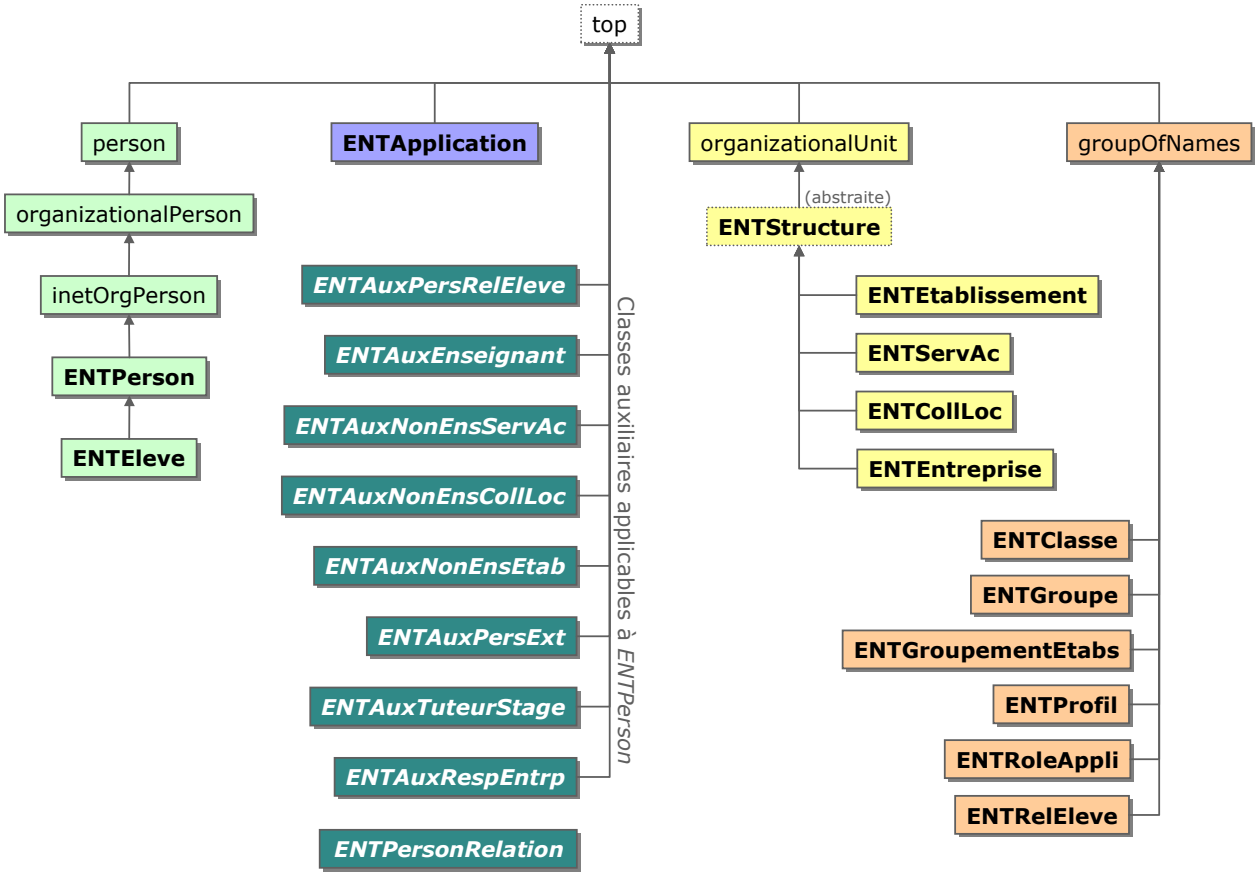

Figure 12 : Schéma LDAP de l'annuaire ENT

4.2.3. Classes relatives aux personnes

4.2.3.1. Classes person, organizationalPerson et inetOrgPerson

Les classes *person*, *organizationalPerson* et *inetOrgPerson* sont des classes LDAP standard qui servent de base pour décrire des personnes. Les attributs correspondants sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Une ligne barrée dans les tableaux ci-dessous indique un attribut présent pour des raisons de rétrocompatibilité. Cet attribut ne devrait pas faire partie de la structure de l'annuaire ENT. Notons qu'il pourra être supprimé dans une future mise à jour majeure du cahier des charges.

Les cellules en italique correspondent à des contraintes spécifiques à l'annuaire ENT sur les propriétés des attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.
Exemple : le standard LDAP autorise l'attribut « telephoneNumber » à être multi-valué alors que dans le modèle de l'annuaire ENT cet attribut doit être mono-valué.

C.[10]	Attribut LDAP	Description	Obl / Fac[11]	Mo / Mu[12]
person	cn	Nom canonique de l'objet	Obl	*Mo*
	sn	Nom d'usage	Obl	*Mo*
	userPassword	Mot de passe de connexion à l'ENT	*Obl*	*Mo*
	seeAlso			
	description			
	telephoneNumber	Numéro de téléphone fixe professionnel	Fac	*Mo*
organizationalPerson	title	Titre	Fac	*Mo*
	x121Address			
	registeredAddress			
	destinationIndicator			
	preferredDeliveryMethod			
	telexNumber			
	telexTerminalIdentifier			
	internationaliSDNNumber			
	facsimileTelephoneNumber	Numéro de fax professionnel	Fac	*Mo*
	street			
	postOfficeBox			
	postalCode			
	postalAddress			
	physicalDeliveryOfficeName			
	ou			
	st			
	l			
inetOrgPerson	audio			
	businessCategory			
	carLicense			

[10] C. : classe LDAP.
[11] Obl / Fac : indique si l'attribut doit obligatoirement être renseigné (Obl) ou s'il peut être laissé vide (Fac).
[12] Mo / Mu : indique si l'attribut est mono-valué (Mo) ou multi-valué (Mu).

C.[10]	Attribut LDAP	Description	Obl / Fac[11]	Mo / Mu[12]
	departmentNumber			
	displayName	Nom et prénom accentués	*Obl*	*Mo*
	employeeNumber			
	employeeType			
	givenName	Prénom usuel	*Obl*	*Mo*
	homePhone	Numéro de téléphone fixe personnel	Fac	*Mo*
	homePostalAddress			
	Initials			
	jpegPhoto	Photographie	Fac	*Mo*
	labeledURI			
	mail	Adresse e-mail	Fac	*Mu*
	manager			
	Mobile	Numéro de téléphone mobile	Fac	*Mu*
	o			
	pager			
	photo			
	roomNumber	Numéro de bureau	Fac	*Mo*
	secretary			
	uid	Identifiant interne à l'ENT	*Obl*	*Mo*
	userCertificates			
	x500UniqueIdentifier			
	preferredLanguage			
	userSMIMECertificate			
	userPKCS12			

Les classes *person*, *organizationalPerson* et *inetOrgPerson* ne doivent pas être instanciées dans l'annuaire ENT.

4.2.3.2. Classe ENTPerson

La classe *ENTPerson* hérite de la classe *inetOrgPerson* et ajoute les attributs communs à toutes les personnes de l'ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
personalTitle	Civilité	Fac	*Mo*
ENTPersonAutresPrenoms	Autres prénoms que le prénom usuel	Fac	Mu
ENTPersonNomPatro	Nom de famille, de naissance (anciennement appelé nom patronymique)	Fac	Mo
ENTPersonSexe	Sexe	Fac	Mo
ENTPersonCentresInteret	Centres d'intérêt par établissement	Fac	Mu
ENTPersonAdresse	Adresse personnelle - champ libre	Fac	Mo
ENTPersonCodePostal	Adresse personnelle - code postal	Fac	Mo
ENTPersonVille	Adresse personnelle - ville	Fac	Mo
ENTPersonPays	Adresse personnelle - pays	Fac	Mo
ENTPersonAdresseDiffusion	Autorisation de diffusion de l'adresse postale et de l'adresse de messagerie aux associations de parents d'élèves siégeant en conseil d'administration	Fac	Mo
ENTPersonLogin	Login (identifiant de connexion à l'ENT)	Obl	Mo
ENTPersonAlias	Alias	Fac	Mo

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTPersonJointure	Clés de jointure	Obl	Mu
GARPersonIdentifiant	Identifiant de la personne pour faire la jointure avec le GAR - à générer par l'ENT	Fac	Mo
ENTPersonStructRattach	Structure de rattachement	Fac	Mo
ENTPersonFonctions	Fonctions et disciplines de poste associées dans des structures	Fac	Mu
ENTPersonDateNaissance	Date de naissance	Fac	Mo
ENTPersonAutresMails	Autres adresses e-mails	Fac	Mu
ENTPersonAutresMobiles	Autres numéros de téléphone mobile	Fac	Mu
ENTPersonMailDiffusion	Adresse e-mail autorisée pour diffusion aux associations de parents d'élèves siégeant en conseil d'administration	Fac	Mo
ENTPersonMobileSMS	Numéro de téléphone mobile autorisé pour l'envoi de SMS	Fac	Mo
ENTPersonProfils	Profils applicatifs associés	Fac	Mu

L'attribut « ENTPersonProfils » doit être mis à jour lors de l'attribution ou du retrait d'un profil applicatif à une personne.

L'attribut « ENTPersonFonctions » doit être utilisé pour déterminer l'ensemble des établissements d'exercices d'un enseignant, l'attribut « ENTPersonStructRattach » fournissant uniquement l'établissement de rattachement administratif de l'enseignant.

Dans le cas où l'attribut « ENTPersonFonctions » est alimenté par le SI du ministère en charge de l'Agriculture, une attention particulière doit être portée à la nomenclature spécifique utilisée : N_FAMILLE_POSTE_EA (cf. annexe Interopérabilité).

Les attributs « ENTPersonAutresMails » et « ENTPersonAutresMobiles » doivent être utilisés pour laisser la possibilité aux utilisateurs de l'ENT de renseigner directement leurs coordonnées personnelles (adresse e-mail, numéro de téléphone mobile) dans l'ENT. Le stockage de ces informations dans ces champs a pour but de ne pas écraser les données de même type (attributs « mail » et « mobile ») qui doivent être uniquement alimentées par des flux automatisés.

La classe *ENTPerson* peut être complétée par une ou plusieurs des classes auxiliaires définies dans le modèle. Ces classes auxiliaires sont détaillées dans la suite du chapitre.

4.2.3.3. Classe ENTEleve

La classe *ENTEleve* hérite de la classe *ENTPerson* et ajoute les attributs relatifs à la catégorie de personnes « Élèves ». Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTElevePersRelEleve	Personne(s) en relation avec l'élève avec les « codes » type de relation, responsable financier, responsable légal, contact, beneficiaire ; Ces codes sont issus de SIECLE (ex-SCONET) sur la base de la table BCN N_LIEN_ELEVE_RESPONSABLE qui remplace la table N_LIEN_PARENTE Pour l'enseignement agricole, ces codes sont calculés sur la base des informations dans Libellule	Fac	Mu
ENTEleveINE	Identifiant national élève (INE)	Fac	Mo
ENTEleveBoursier	Boursier	Fac	Mo
ENTEleveRegime	Régime établissement de rattachement	Fac	Mo

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEleveAdresseRel	Adresses de résidence (chez un représentant légal ou personne en charge)	Fac	Mu
ENTEleveTransport	Transport scolaire	Fac	Mo
ENTEleveStatutEleve	"Statut" de l'élève	Obl	Mo
ENTEleveMEF	MEF	Obl	Mo
ENTEleveLibelleMEF	Libellé MEF	Obl	Mo
ENTEleveNivFormation	Niveau de formation	Obl	Mo
ENTEleveFiliere	Filière	Obl	Mo
ENTEleveNivFormationDiplome	Niveau de formation du diplôme	Fac	Mo
ENTEleveSpecialite	Spécialité	Fac	Mo
~~ENTEleveEnseignements~~	~~Enseignements~~	~~Fac~~	~~Mu~~
ENTEleveCodeEnseignements	Code des enseignements	Fac	Mu
ENTEleveStructRattachId	Identifiant de l'élève dans SIECLE	Obl	Mo
ENTEleveClasses	Établissements et classe associée	Obl	Mu
ENTEleveGroupes	Établissements et groupes associés	Fac	Mu
ENTEleveEnsRespStage	Enseignant responsable de stage	Fac	Mo
ENTEleveEnsTutStage	Enseignants tuteurs de stage	Fac	Mu
ENTEleveEntrTutStage	Tuteur de stage / Maître d'apprentissage	Fac	Mo
ENTEleveEntrAutres	Autres personnes de l'entreprise suivant l'élève en stage	Fac	Mu
ENTEleveDelegClasse	Élève délégué de classe	Fac	Mo
ENTEleveDelegAutres	Élève délégué autres	Fac	Mu
ENTEleveMajeur	Majeur	Obl	Mo
ENTEleveMajeurAnticipe	Majeur anticipé	Fac	Mo

L'attribut « ENTEleveClasses » doit être utilisé pour déterminer l'ensemble des établissements d'un élève, l'attribut « ENTPersonStructRattach » fournissant uniquement l'établissement de rattachement administratif de l'élève.

4.2.3.4. Classe ENTAuxPersRelEleve

La classe *ENTAuxPersRelEleve* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Personnes en relation avec les élèves*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxPersRelEleveEleve	Identifiant(s) de(s) élève(s) avec qui la personne est en relation	Obl	Mu
ENTAuxPersRelEleveRepresentant	Représentant des parents d'élèves	Fac	Mu

La classe auxiliaire *ENTAuxPersRelEleve* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.5. Classe ENTAuxEnseignant

La classe *ENTAuxEnseignant* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Enseignants*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxEnsCategoDiscipline	Catégories de discipline de poste	Fac	Mu

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxEnsMEF	Codes MEF et libellé associé pour chaque établissement	Fac	Mu
ENTAuxEnsMatiereEnseignEtab	Établissement et matières enseignées	Fac	Mu
~~ENTAuxEnsClasses~~	~~Établissement et classes associées~~	~~Fac~~	~~Mu~~
~~ENTAuxEnsGroupes~~	~~Établissement et groupes associés~~	~~Fac~~	~~Mu~~
ENTAuxEnsClassesPrincipal	Établissement et classe associée dont la personne est professeur principal	Fac	Mu
ENTAuxEnsRespStage	Élèves stagiaires en responsabilité	Fac	Mu
ENTAuxEnsTutStage	Élèves stagiaires suivis	Fac	Mu
ENTAuxEnsClassesMatieres	Lien Établissement / Divisions / codes matières enseignées dans division	Fac	Mu
ENTAuxEnsGroupesMatieres	Lien Établissement / Groupes / codes matières enseignées dans groupe	Fac	Mu

La classe auxiliaire *ENTAuxEnseignant* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

L'attribut ENTAuxEnsCategoDiscipline fournit des codes pivots pour les disciplines d'enseignements uniquement. Il n'existe pas de pivots pour les autres fonctions.

4.2.3.6. Classe ENTAuxNonEnsServAc

La classe *ENTAuxNonEnsServAc* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement aux services académiques*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsServAcService	Service	Fac	Mo
ENTAuxNonEnsServAcDomaineEtab	Établissements d'exercice et domaines associés	Fac	Mu
ENTAuxNonEnsServAcDomaineRegroupEtabs	Regroupement d'établissements d'exercice et domaines associés	Fac	Mu

La classe auxiliaire *ENTAuxNonEnsServAc* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.7. Classe ENTAuxNonEnsCollLoc

La classe *ENTAuxNonEnsCollLoc* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement à une collectivité locale*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsCollLocService	Service	Fac	Mo
ENTAuxNonEnsCollLocDomaineEtab	Établissements d'exercice et domaines associés	Fac	Mu

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsCollLocDomaineRegroupEtabs	Regroupement d'établissements d'exercice et domaines associés	Fac	Mu

La classe auxiliaire *ENTAuxNonEnsCollLoc* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.8. Classe ENTNonEnsEtab

La classe *ENTAuxNonEnsEtab* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Non enseignants rattachés administrativement à un établissement d'enseignement*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxNonEnsEtabService	Service	Fac	Mo

La classe auxiliaire *ENTAuxNonEnsEtab* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.9. Classe ENTAuxPersExt

La classe *ENTAuxPersExt* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Personnels extérieurs*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxPersExtService	Service	Fac	Mo

La classe auxiliaire *ENTAuxPersExt* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.10. Classe ENTAuxTuteurStage

La classe *ENTAuxTuteurStage* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Tuteurs de stage et maîtres d'apprentissage*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxTuteurStageSociete	Société	Obl	Mo
ENTAuxTuteurStageEleves	Élevés suivis en stage ou en apprentissage	Obl	Mu

La classe auxiliaire *ENTAuxTuteurStage* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.11. Classe ENTAuxRespEntrp

La classe *ENTAuxRespEntrp* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la catégorie de personnes *Responsables des entreprises partenaires*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTAuxRespEntrpSociete	Société	Obl	Mo

La classe auxiliaire *ENTAuxRespEntrp* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.3.12. Classe ENTPersonRelation

La classe *ENTPersonRelation* est une classe auxiliaire permettant de compléter la classe *ENTPerson* avec les attributs relatifs à la définition des opérations de réconciliation entre comptes utilisateurs. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTPersRelRapprochPrincipal	Compte principal rattaché	Fac	Mo
ENTPersRelRapprochSecondaire	Compte secondaire rattaché	Fac	Mu
ENTPersRelFusionPrincipal	Compte principal fusionné	Fac	Mo
ENTPersRelFusionSecondaire	Compte secondaire fusionné	Fac	Mu

Les attributs « ENTPersRelFusionPrincipal » et « ENTPersRelFusionSecondaire » sont essentiellement utilisés pour permettre un retour arrière et annuler une opération de fusion effectuée par erreur.

La classe auxiliaire *ENTPersonRelation* ne doit compléter que des objets appartenant à la classe *ENTPerson*.

4.2.4. Classes relatives aux structures

4.2.4.1. Classe organizationalUnit

La classe *organizationalUnit* est une classe LDAP standard qui sert de base pour décrire des structures. Les attributs sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ou			
description			
preferredDeliveryMethod			
searchGuide			
st			
businessCategory			
telexNumber			
l	Adresse professionnelle - ville	Fac	*Mo*
seeAlso			
telephoneNumber	Numéro de téléphone	Fac	*Mo*
physicalDeliveryOfficeName			
postalCode	Adresse professionnelle - code postal	Fac	*Mo*
internationalISDNNumber			
x121Address			
userPassword			

Attribut LDAP	Description	Obl / Fac	Mo / Mu
registeredAddress			
Street	Adresse professionnelle - champ libre	Fac	*Mo*
postalAddress			
facsimileTelephoneNumber	Numéro de fax	Fac	*Mo*
teletexTerminalIdentifier			
postOfficeBox	Adresse professionnelle - boîte postale	Fac	*Mo*
destinationIndicator			

4.2.4.2. Classe ENTStructure

La classe *ENTStructure* est une classe abstraite qui hérite de la classe *organizationalUnit* et la complète avec les attributs communs à toutes les structures de l'ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTStructureJointure	Nom courant / Raison sociale	Obl	Mu
ENTStructureTypeStruct	Type de structure	Fac	Mo
ENTStructureNomCourant	Nom courant / Raison sociale	Obl	Mo
ENTStructureResponsable	Responsable	Fac	Mo
ENTStructureSIREN	Numéro de SIREN / SIRET	Fac	Mo
ENTStructureEmailSI	Adresse e-mail dans le SI non modifiable	Fac	Mo
ENTStructureEmail	Adresse e-mail	Fac	Mo
ENTStructureSiteWeb	Site web	Fac	Mo
ENTStructureContactENT	Contact ENT	Fac	Mo
ENTStructureUAI	Numéro UAI	Fac	Mo

La classe abstraite *ENTStructure* ne peut pas être instanciée.

4.2.4.3. Classe ENTEtablissement

La classe *ENTEtablissement* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Établissements d'enseignement*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEtablissementMinistereTutelle	Ministère de tutelle	Obl	Mo
ENTEtablissementContrat	Contrat	Obl	Mo
ENTEtablissementStructRattachAdmin	Structures de rattachement administratif	Fac	Mu
ENTEtablissementStructRattachFctl	Structures de rattachement fonctionnel	Fac	Mu
ENTEtablissementBassin	Bassin de formation	Fac	Mo
ENTStructureClasses	Liste des divisions (code et libellé) et Mef associés	Fac	Mu
ENTStructureGroupes	Liste des groupes (code et libellé) et divisions d'appartenance	Fac	Mu

Les caractéristiques des attributs notés « en attente » dans l'annexe 4bis feront l'objet d'une confirmation au moment de leur livraison par AAF.

4.2.4.4. Classe ENTServAc

La classe *ENTServAc* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Services académiques*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTServAcAcademie	Académie	Obl	Mo

4.2.4.5. Classe ENTCollLoc

La classe *ENTCollLoc* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Collectivité locale*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTCollLocLieuGeographique	Région ou département	Obl	Mo

4.2.4.6. Classe ENTEntreprise

La classe *ENTEntreprise* complète la classe *ENTStructure* avec les attributs relatifs à la catégorie de structures *Entreprises partenaires*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTEntrepriseEtabs	Établissements partenaires	Obl	Mu

4.2.5. Classes relatives aux groupes d'entrées de l'annuaire ENT

4.2.5.1. Classe groupOfNames

La classe *groupOfNames* est une classe LDAP standard qui sert de base pour décrire des groupes d'entrées de l'annuaire ENT (groupes de personnes, de structures, de groupes…). Les attributs correspondants sont donnés dans le tableau ci-dessous.

Les attributs grisés ne sont pas utilisés par le modèle d'information de l'annuaire ENT.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
cn	Nom du groupe	Obl	*Mo*
businessCategory			
seeAlso			
owner	Propriétaire(s) du groupe	Fac	*Mu*
ou			
o			
description	Description du groupe	Fac	*Mo*

Attribut LDAP	Description	Obl / Fac	Mo / Mu
member	Membres du groupe	Fac	Mu

4.2.5.2. Classe ENTClasse

Remarque : il est ici question de la « classe LDAP » représentant une « classe d'élèves ».

La classe ENTClasse hérite de la classe groupOfNames et ajoute les attributs relatifs aux classes des élèves. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe ENTClasse*)*			

Les classes sont définies par établissement d'enseignement. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement pour lequel est définie la classe.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des élèves de la classe.

L'attribut « cn » doit désigner de façon unique une classe sur le périmètre de l'ENT. La règle de construction proposée est la suivante : le nom d'une classe doit être préfixé du numéro SIREN de l'établissement d'enseignement pour lequel elle est définie, suivi d'un « _ ».
Exemple : `123456789_3eme2`

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement définir sa propre règle de construction.

4.2.5.3. Classe ENTGroupe

La classe *ENTGroupe* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux groupes d'élèves. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe ENTGroupe*)*			

Les groupes d'élèves sont définis par établissement d'enseignement. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement pour lequel est défini le groupe.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des élèves du groupe.

L'attribut « cn » doit désigner de façon unique un groupe d'élèves sur le périmètre de l'ENT. La règle de construction proposée est la suivante : le nom du groupe d'élèves peut être préfixé du numéro SIREN pour lequel il est défini, suivi d'un « _ ».
Exemple : `123456789_latin2`

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement définir sa propre règle de construction.

4.2.5.4. Classe ENTGroupementEtabs

La classe *ENTGroupementEtabs* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux groupements d'établissements (bassins de formation, cités scolaires, GRETA). Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe ENTGroupementEtabs*)*			

L'attribut « owner », hérité de *groupOfNames*, n'est pas renseigné. Le porteur pourra préciser cet attribut s'il le souhaite.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des établissements qui constituent le regroupement.

L'attribut « cn » doit désigner de façon unique un groupement d'établissements sur le périmètre de l'ENT.

4.2.5.5. Classe ENTProfil

La classe *ENTProfil* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux profils applicatifs décrits dans le modèle de sécurité de l'annuaire ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTProfilPeuplement	Règle de peuplement	Fac	Mo

Il existe deux types de profils applicatifs :

- les profils applicatifs partagés au niveau du projet et qui sont donc transverses aux établissements d'un ENT ; dans ce cas, l'attribut « owner », hérité de *groupOfNames*, n'est pas renseigné) ;
- les profils applicatifs locaux définis sur le périmètre d'une structure (établissement notamment) ; dans ce cas, l'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de l'établissement d'enseignement qui a défini le profil applicatif.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des personnes associées à ce profil applicatif.

L'attribut « cn » doit désigner de façon unique un groupement d'établissements sur le périmètre de l'ENT. La règle de construction est la suivante :

- les profils applicatifs partagés au niveau projet sont préfixés par le code projet ENT : « `LxxCiiii` »
- les profils applicatifs définis par des structures sont préfixés par le numéro UAI de la structure suivi de « _ ».

Des informations complémentaires sur les règles de peuplement des profils applicatifs sont données au chapitre 3.2.

4.2.5.6. Classe ENTRoleAppli

La classe *ENTRoleAppli* hérite de la classe *groupOfNames* et ajoute les attributs relatifs aux rôles applicatifs décrits dans le modèle de sécurité de l'annuaire ENT. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTRoleAppliProfils	Profils applicatifs associés	Fac	Mu

Un rôle applicatif est défini par rapport à une ou plusieurs applications données. L'attribut « owner », hérité de *groupOfNames*, correspond au « dn » de ou des applications qui ont défini le rôle applicatif. Cet attribut doit nécessairement être renseigné.

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » des personnes associées à ce rôle applicatif.

4.2.5.7. Classe ENTRelEleve

La classe *ENTRelEleve* hérite de la classe *groupOfNames* et ajoute les attributs relatifs à une relation entre un *Élève* et une *Personne en relation avec l'élève*. Ces attributs sont donnés dans le tableau ci-dessous.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
(aucun attribut supplémentaire pour la classe ENTRelEleve*)*			

L'attribut « member », hérité de *groupOfNames*, correspond aux « dn » d'un seul *Eleve* et d'une seule *Personne en relation avec l'élève*.

L'attribut « description », hérité de *groupOfNames*, qualifie la relation entre l'*Eleve* et la *Personne en relation avec l'élève*.

Remarque : Il est nécessaire de créer un groupe par relation que l'on veut représenter.

4.2.6. Classe relative aux applications

4.2.6.1. Classe ENTApplication

La classe *ENTApplication* hérite directement de la classe *top* et décrit les applications qui utilisent l'annuaire ENT. Ces applications peuvent reposer ou non sur le socle ENT. Les attributs sont donnés dans le tableau ci-dessous.

Les cellules en italique correspondent à des restrictions spécifiques à l'annuaire ENT sur les propriétés d'attributs. Ces contraintes d'intégrité devront être contrôlées par les services de gestion de contenu en plus de celles mentionnées au chapitre 3.3.

Attribut LDAP	Description	Obl / Fac	Mo / Mu
ENTApplicationId	Identifiant	Obl	Mo
userPassword	Mot de passe	Obl	*Mo*
ENTApplicationNom	Nom	Obl	Mo
ENTApplicationDesc	Description	Fac	Mo
ENTApplicationCatego	Catégorie	Obl	Mu
ENTApplicationProprietaire	Propriétaire de l'application	Fac	Mo
ENTApplicationProfils	Profils utilisés par l'application	Fac	Mu
ENTApplicationRolesAppli	Rôles applicatifs utilisés par l'application	Fac	Mu

La classe *ENTApplication* possède un identifiant et un mot de passe qui permettent à l'annuaire ENT d'authentifier l'application sur l'ENT.

4.3. DIT de l'annuaire ENT

4.3.1. Racine

La maîtrise d'ouvrage en charge du projet ENT indiquera la racine qu'il souhaite mettre en place pour l'annuaire ENT. La seule contrainte est de faire référence au nom du projet ENT dans la racine.

Exemple de racine possible pour le projet PRISME : « `dc=prisme-lorraine, dc=net` »

4.3.2. Arborescence

L'organisation retenue pour le DIT est une organisation à plat. Dans cette organisation, tous les objets de l'annuaire ENT sont classés dans des catégories directement rattachées à la racine.

Les catégories sont :

- *personnes* : liste des personnes, contient des objets des classes *ENTPerson* et *ENTEleve* ;
- *structures* : liste des structures, contient des objets des classes ENTEtablissement, ENTServAc, ENTCollLoc et ENTEntreprise ;
- *groupes* : liste des groupes, contient les objets des classes ENTClasse, ENTGroupe, ENTGroupementEtabs, ENTProfil, ENTRoleAppli et ENTRelEleve ;
- *applications* : liste des applications utilisant l'annuaire ENT, contient les objets de la classe *ENTApplication*.

Des contraintes applicatives, notamment par rapport aux services AAS, pourraient imposer d'utiliser des termes anglais pour les branches personnes (people) *et groupes (*groups*). La maîtrise d'ouvrage en charge du projet ENT modifiera en conséquence le DIT de l'annuaire ENT ou laissera éventuellement cette liberté au soumissionnaire.*

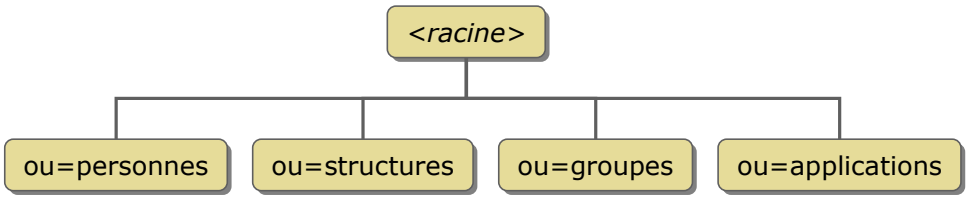

Figure 13 : DIT de l'annuaire ENT

Compte tenu du nombre de personnes au sein de l'ENT, les risques d'homonymie sont très présents. C'est pourquoi l'attribut « cn », tel qu'il est construit, ne pourra pas être utilisé comme RDN (*Relative Distinguished Name*) des personnes. Des précisions sont données au chapitre 4.4.

Le soumissionnaire pourra proposer et justifier une organisation plus hiérarchique en précisant les impacts éventuels sur le schéma et notamment comment les personnes exerçant dans plusieurs établissements sont alors gérées (cf. chapitre 4.2.1). Il précisera également si des ACL sont positionnées sur certaines branches.

4.4. Attributs particuliers

4.4.1. Identifiant unique des personnes sur l'annuaire ENT

Toute entrée appartenant à la classe *inetOrgPerson* ou à une classe qui en hérite possède un attribut « uid ». Cet attribut représente l'identifiant interne à l'ENT et doit être unique sur le périmètre national.

4.4.1.1. Format de l'identifiant unique

Un format d'identifiant unique qui ne permette pas d'être associé à l'identité de l'accédant doit être proposée. À défaut, la méthode suivante peut être utilisée :

Cet identifiant est de la forme «LxxCjjMMaahhmmsszzz» avec :

- L et C correspondent aux codes de la maîtrise d'ouvrage en charge du projet ENT ; (cf. le §4.2 de l'annexe opérationnelle SDET)
- xx : 2 lettres à générer pour chaque entrée ;
- jjMMaahhmmsszzz : 15 chiffres à générer pour chaque entrée à partir de la date de création de l'identifiant opaque ou du compte utilisateur à la milliseconde avec :
  - jj : jour de création sur deux caractères ;
  - mm : mois de création sur deux caractères ;
  - aa : année de création sur deux caractères ;
  - hh : heure de création sur deux caractères ;
  - ss : seconde de création sur deux caractères ;
  - zzz : milliseconde de création sur trois caractères.

4.4.1.2. Service de génération de l'identifiant

Dans les cas où la méthode proposée ci-dessus serait retenue pour la génération de l'identifiant, un service de génération de l'identifiant serait à implémenter suivant les principes de fonctionnement suivants :

- respect du format présenté ;
- utilisation du code projet ENT pour les caractères L et C ;
- génération des caractères xx sur la base des attributs discriminants suivants :
  - le nom d'usage,
  - le prénom usuel (les attributs complémentaires suivants peuvent être utilisés pour résoudre les cas d'homonymie (deux personnes possédant les mêmes valeurs pour tous les attributs discriminants),
  - les autres prénoms,
  - le nom de famille (patronymique) ;
- utilisation de la date de création du compte à la milliseconde pour les caractères jjMMaahhmmsszzz (le projet ENT veillera au respect de ce principe également dans le cas d'une création des comptes par lots) ;
- renvoi de l'identifiant déjà généré si les mêmes attributs discriminants sont présentés.

La maîtrise d'ouvrage en charge du projet ENT déterminera si l'identifiant d'un utilisateur supprimé peut être réutilisé, et si oui, au bout de combien de temps. Notons que la réutilisation d'un identifiant peut présenter un risque de confusion d'identité vis-à-vis d'un tiers.

4.4.2. Login

Toute entrée appartenant à la classe *ENTPerson* ou à une classe qui en hérite possède un attribut « ENTPersonLogin » qui correspond à l'identifiant de connexion à l'ENT.

Cet identifiant de connexion doit être unique sur le périmètre de l'ENT. Cette unicité doit également prendre en compte les valeurs d'alias existants (cf. chapitre suivant).

La maîtrise d'ouvrage en charge du projet ENT pourra supprimer la phrase précédente si la fonctionnalité d'alias n'est pas proposée.

4.4.2.1. Format du login

La maîtrise d'ouvrage en charge du projet ENT pourra choisir parmi les propositions suivantes la règle de construction du login qu'elle souhaite adopter : prenom.nomXX, où XX est un incrément garantissant l'unicité, pnomXX, où XX est un incrément garantissant l'unicité, autre proposition.

Remarque : dans le cas où le login se repose en partie sur le nom, il est conseillé de ne pas positionner le champ « ENTPersonLogin » comme attribut utilisé pour définir l'identifiant unique de l'utilisateur (son « dn » dans l'annuaire LDAP), afin de gérer plus facilement les changements de nom.

4.4.2.2. Service de génération du login

Selon le format de login choisi par la maîtrise d'ouvrage en charge du projet ENT, un service de génération du login peut être nécessaire (notamment en cas d'incrément garantissant l'unicité). La maîtrise d'ouvrage en charge du projet ENT indiquera ici les principes de fonctionnement attendus pour ce service.

4.4.3. Alias

Le schéma LDAP proposé permet de créer un seul alias pour chaque utilisateur. Il devra être adapté si la maîtrise d'ouvrage en charge du projet ENT ne souhaite pas offrir cette fonctionnalité, ou souhaite que les utilisateurs disposent de plusieurs alias.

Ce chapitre pourra être supprimé si la maîtrise d'ouvrage en charge du projet ENT ne souhaite pas offrir cette fonctionnalité.

Toute entrée appartenant à la classe *ENTPerson* ou à une classe qui en hérite possède un attribut « ENTPersonAlias » qui correspond à un identifiant alternatif de connexion à l'ENT. Celui-ci peut donc être utilisé à la place de « ENTPersonLogin ».

L'alias offre aux utilisateurs la possibilité de choisir un identifiant de connexion plus facile à retenir que celui qui est fourni automatiquement. La règle de création de l'alias est la suivante : un alias donné est attribué à la première personne qui en fait la demande.

Cet alias doit être unique sur le périmètre de l'ENT. Cette unicité doit également prendre en compte les valeurs des identifiants de connexion existants (cf. chapitre précédent).

Remarque : Le fait d'utiliser un alias a pour avantage de gérer plus facilement les changements de nom, sans impacter le « dn » de l'utilisateur

La maîtrise d'ouvrage en charge du projet ENT pourra définir, si elle le souhaite, des contraintes s'appliquant sur le format des alias.

Le service permettant à un utilisateur de se créer un alias est décrit au chapitre 6.1.2.

4.4.4. « cn » des personnes

Le *Common Name*, ou « cn », des utilisateurs est construit comme suit :

- nom d'usage (en majuscules sans caractères diacritiques) ;
- suivi d'un espace ;
- suivi du prénom usuel (en minuscule, sauf la première lettre, et avec caractères diacritiques).

Les lettres entrelacées sont séparées et les traits d'union et les apostrophes sont remplacés par des espaces.

Exemple : *DE LA FONTAINE Jean Pierre*

Remarque : L'unicité d'un « cn » dans la branche *people* n'est pas garantie. Il ne sera donc pas utilisé dans la construction du « dn ».

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement proposer une autre règle de construction du « cn ».

4.4.5. Photographie

Toute entrée appartenant à la classe *inetOrgPerson* ou à une classe qui en hérite possède un attribut « jpegPhoto ». Cet attribut permet de stocker une photographie au format JPEG ; il n'est utilisé que pour certaines catégories de personnes.

Le stockage de ces photographies au sein de l'ENT représente un volume de données conséquent qui peut impacter fortement les performances de l'annuaire ENT.

Des indications volumétriques sont données au chapitre 7. À partir de ces informations, le soumissionnaire indiquera s'il est préférable de stocker les photographies dans l'annuaire ENT ou au sein d'un support de stockage externe.

Dans le deuxième cas, l'annuaire ENT ne conservera que le chemin permettant d'accéder au fichier.

Dans tous les cas, un contrôle sur la taille maximum des photographies sera nécessaire.

4.4.6. Construction du « dn »

Chaque entrée de l'annuaire est référencée de manière unique dans le DIT par son « dn » (*Distinguished Name*). Il s'agit du chemin d'accès à l'entrée depuis le sommet de l'arbre.

La construction du « dn » est la suivante :

- le « dn » des entrées représentant des personnes sera basé sur l'attribut « uid » ;
- le « dn » des entrées représentant des structures d'établissement sera basé sur l'attribut « ENTStructureUAI » ;
- le « dn » des entrées représentant les autres structures sera basé sur l'attribut « ENTStructureSIREN » ;
- le « dn » des entrées représentant des groupes sera basé sur l'attribut « cn » ;
- le « dn » des entrées représentant des applications sera basé sur l'attribut « ENTApplicationId ».

4.4.7. ENTPersonJointure et ENTStructureJointure (clés de jointure avec les sources autoritaires)

Afin d'assurer la correspondance entre les objets personnes et structures des sources autoritaires et ceux stockés dans l'annuaire ENT, il est nécessaire de disposer d'un identifiant commun jouant le rôle de clé de jointure.

Chaque source autoritaire fournit donc une clé de jointure persistante, qui permet d'identifier de manière unique chaque personne et chaque structure au fil des alimentations successives, et donc de suivre le cycle de vie des objets (modification des attributs et suppression). **Cette clé de jointure doit notamment être pérenne d'une année scolaire sur l'autre.**

Une même entrée personne ou structure dans l'annuaire ENT doit cependant disposer d'une clé de jointure pour chacune des sources autoritaires qui permettent d'alimenter un ou plusieurs de ses attributs.

Les clés de jointure sont stockées dans l'annuaire ENT grâce aux attributs multi-valués « ENTPersonJointure » (pour les personnes) et « ENTStructureJointure » (pour les structures). Ils sont construits comme suit :

- identifiant de la source autoritaire, les identifiants sont les suivants :
  - alimentation manuelle depuis l'ENT : identifiant = « ENT »,
  - alimentation depuis le SI du MEN : identifiant = « AC- » + nom de l'académie,
  - autres sources d'alimentation : identifiant librement défini par chaque projet ENT (par exemple, pour l'enseignement agricole, « EA- » + code académie ou code région) ;
- suivi du caractère « $ » ;
- suivi de la clé de jointure fournie par la source autoritaire pour désigner l'objet.

Remarque : Ce champ est distinct de l'identifiant unique des personnes sur l'annuaire ENT, défini au chapitre 4.4.1.

4.4.8. INE (identifiant national des élèves)

L'arrêté du 30 novembre 2006 modifié par l'arrêté du 13 octobre 2017 portant création, au sein du ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, d'un traitement de données à caractère personnel relatif aux espaces numériques de travail autorise dans les ENT le traitement de l'INE (identifiant national de l'élève). Cet attribut de l'annuaire ENT est alimenté par le SI du MEN et est disponible d'ici la fin de l'année scolaire 2017-2018 pour le second degré.

Cette information sera prochainement disponible pour l'enseignement agricole également.

Cet INE est destiné exclusivement à une utilisation interne au périmètre de l'ENT par exemple pour conserver les données lors du passage du premier degré au second degré, lors d'un changement d'académie à l'intérieur d'un projet ENT ou pour l'interfaçage avec certaines applications nationales sous responsabilité du ministère comme par exemple le livret scolaire (livret scolaire du CP à la 3e) dans le premier degré.

L'INE ne doit pas être utilisé en dehors des finalités autorisées par la CNIL.

4.4.9. GARPersonIdentifiant (identifiant GAR pour les personnes)

Afin de disposer d'une clé de jointure unique et pérenne entre les utilisateurs de l'ENT et le GAR, le projet ENT doit fournir un identifiant unique dédié au GAR, appelé GARPersonIdentifiant :

- pour les élèves ou enseignants qui accèdent aux ressources depuis leur ENT (profils National_ens, National_doc et National_elv) ;
- pour les « responsables d'affectation » (utilisateurs chargés d'affecter les ressources aux élèves et enseignants).

Le GARPersonIdentifiant est transmis au GAR par le projet ENT lors du provisionnement des données du GAR conformément au Référentiel technique, fonctionnel et de sécurité du GAR (RTFS) à destination des éditeurs/intégrateurs ENT (cf. chapitre 6 de l'annexe opérationnelle du SDET).

En cas de changement de solution ENT (par exemple en cas de renouvellement ou de changement de marché ENT), dans le cadre de la reprise de données liée à la réversibilité, cet identifiant doit faire partie de données à reprendre dans la nouvelle solution. La même contrainte s'applique en cas de changement de prestataire ENT ou de modification du périmètre du projet ENT, qu'il y ait un changement de solution ENT ou pas (cf. chapitre 3.4.10 de l'annexe opérationnelle du SDET).

Pour assurer l'unicité de cet identifiant GARPersonIdentifiant sur le périmètre national, la version #4 de l'UUID (RFC4122), aussi connu comme GUID, devrait être utilisée.

La version #4 de l'UUID est généralement disponible en standard dans les principaux langages de programmation, notamment pour Java, à partir de Java 5, et C#, ou en tant que librairies externes.

Le GARPersonIdentifiant devrait être stocké dans l'annuaire de l'ENT sur 32 caractères en base-16

Divers aspects techniques sont à prendre en compte :

- Format de transmission : l'UUID se présente et se transmet habituellement sous la forme de chaîne de 36 caractères (32 caractères hexadécimaux en 5 groupes séparés par des tirets), tel que c'est utilisé dans la RFC 4122, que ce soit en JSON ou en XML. S'il s'agit de transmettre ce type d'identifiant dans des services de type SOAP, le format de transmission devrait être aussi cette chaîne de caractères car le format UUID n'existe pas en tant que tel dans la spécification du protocole. Voici à titre d'exemple, à quoi pourrait ressembler la définition de l'UUID à transmettre dans JSON et XML :
  - En JSON schema :
    - "uuid": {
      "type": "string",
      "pattern": "^[a-fA-F0-9]{8}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{4}-[a-fA-F0-9]{12}$"
      }
  - En *XML* :
    - <s:simpleType name="guid">
      <s:restriction base="s:string">
      <s:pattern value="[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}"/>
      </s:restriction>
      </s:simpleType>
- Format de manipulation (dans le GAR, l'ENT ou autre système connexe) : compte tenu du fait que les principaux langages de programmation représentent souvent les UUID dans le format de chaîne de 36 caractères mentionné, il est conseillé d'utiliser ce format en interne dans les différents systèmes et dans la communication avec le GAR ;
  - en Java, le résultat de l'appel à *toString* sur un objet de type UUID utilise le format mentionné ;
  - en C#, il est possible d'obtenir un objet UUID directement à partir d'un String qui se trouve dans ce format de 36 caractères évoqué. En ce qui concerne l'affichage, la fonction *ToString*[13] permet de produire un UUID au format mentionné à l'aide du spécificateur « D ».
- Format d'affichage (pour debug par exemple) : le format de 36 caractères est souvent jugé le plus adapté car plus facilement lisible pour les humains ;
- Format de stockage en base : au moment de stocker des UUID dans les bases de données, mis à part le stockage sous forme de variable de caractères (VARCHAR), des formats plus adaptés/optimisés peuvent être envisagés pour faciliter l'indexation, comme par exemple le type BINARY(16) dans MySQL ou un format équivalent. Pour information, sur MySQL 8, il y a les fonctions UUID_TO_BIN et BIN_TO_UUID pour transformer des UUID en chaîne de caractères et vice-versa.

[13] ToString (https://msdn.microsoft.com/fr-fr/library/97af8hh4(v=vs.110).aspx)

5. Architecture technique de l'annuaire ENT

Plusieurs exigences et éléments de contexte ont servi à bâtir l'architecture technique de l'annuaire ENT :

- les besoins en termes d'usage de l'annuaire : mise à jour, gestion, authentification / autorisation, consultation ;
- la répartition géographique des sources d'alimentation, notamment celles du MEN ;
- le périmètre minimum couvert par un ENT (à savoir un département) ;
- la volumétrie attendue.

Sur la base de ces éléments, une solution d'architecture a été définie. Cette architecture est présentée en détails au chapitre 5.1.

Cette solution peut être déclinée en trois options afin de garantir des niveaux de disponibilité et de partage de charge en adéquation avec les exigences de qualité de service.

Le soumissionnaire préconisera l'option la plus pertinente au regard de son offre technique et des éléments de volumétrie présentés au chapitre 7. Par défaut, l'option à retenir sera la première.

La maîtrise d'ouvrage en charge du projet ENT pourra cependant choisir d'imposer une des options aux soumissionnaires.

5.1. Principes d'architecture

La solution d'architecture (Figure 14) repose sur la séparation de l'annuaire ENT en deux référentiels typés par usage :

- un référentiel pour les mises à jour, la gestion et la consultation d'informations ;
- un référentiel pour l'authentification et l'autorisation des utilisateurs.

Quelques éléments de justification :

- les performances du référentiel d'authentification et d'autorisation ne sont pas impactées par les requêtes de consultation et les accès en écriture lors des mises à jour ;
- cette séparation permet d'appliquer des procédures d'exploitation adaptées aux exigences de qualité de service de chacun des référentiels (plus fortes pour un référentiel d'authentification / autorisation que pour un référentiel de consultation).

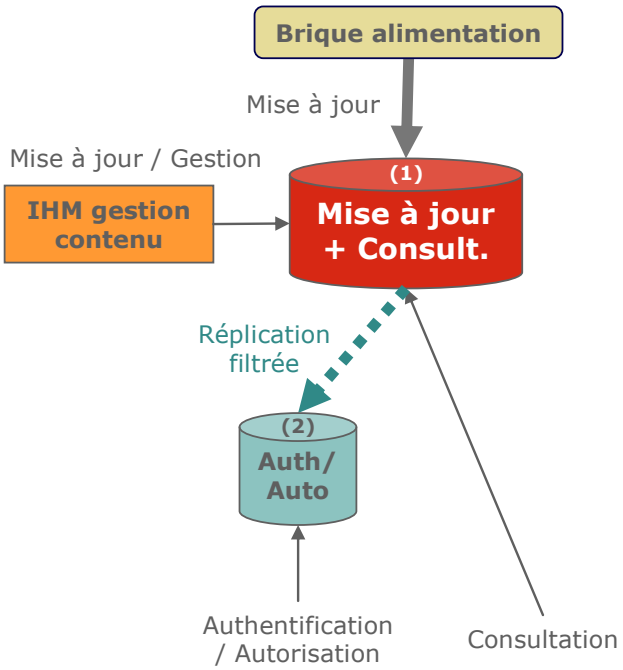

Figure 14 : Solution d'architecture de l'annuaire ENT

La brique d'alimentation correspond au composant technique du service d'alimentation chargé de la mise à jour automatique de l'annuaire ENT (cf. chapitre 6.1.1). Les mises à jour depuis cette brique, ainsi que les mises à jour manuelles depuis l'IHM de gestion de contenu, sont réalisées sur le référentiel (1). Celui-ci traite également les requêtes de consultation, en provenance des applications.

Le référentiel (2) est dédié aux requêtes d'authentification et d'autorisation. Il est alimenté par réplication filtrée depuis le référentiel (1). Seuls les attributs utiles à la gestion des autorisations sont répliqués dans le référentiel (2).

5.1.1. Indexation de l'annuaire ENT

Afin d'améliorer le temps de réponse aux requêtes effectuées sur l'annuaire ENT, des index doivent être créés sur certains attributs.

Le référentiel de « mise à jour, gestion et consultation » et le référentiel « d'authentification / autorisation » pourront disposer d'index différents.

Il est notamment recommandé de créer des index sur les attributs suivants : « uid », « login », « alias », « ENTPersonStructRattach ».

1.1. Architecture – option 1

La première option (Figure 15) correspond à une mise en œuvre minimaliste de la haute-disponibilité sur la solution d'architecture présentée précédemment.

La haute-disponibilité repose sur la mise en place d'un référentiel (1') de secours. Il s'agit d'une réplication totale du référentiel (1) de mise à jour et de consultation.

Les applications ne s'adressent qu'à un proxy LDAP (ou un commutateur de niveau 7/Applicatif) dont le rôle est de répartir les requêtes en fonction de leur type :

- les requêtes de consultation sont dirigées vers le référentiel (1) ;

- les requêtes d'authentification / autorisation sont dirigées vers le référentiel (2).

Remarque : Un proxy LDAP offre cependant des fonctions plus avancées permettant d'optimiser les performances (ex. : gestion de cache).

Si un des référentiels (1) ou (2) ne répond pas, le proxy LDAP (ou le commutateur de niveau 7) redirige les requêtes vers le référentiel (1') de secours.

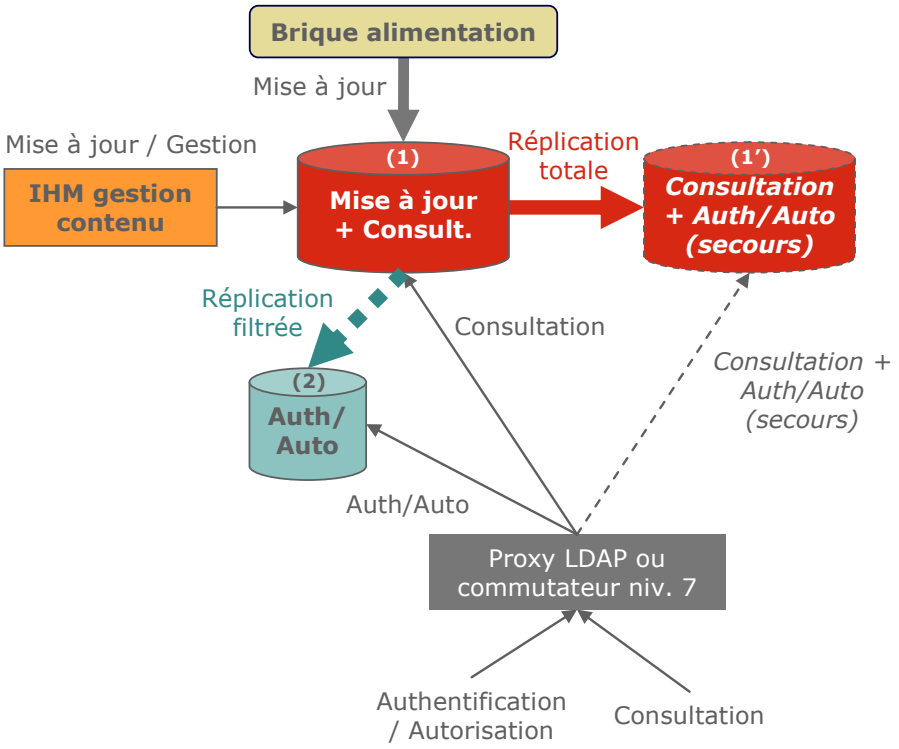

Figure 15 : Architecture – Option 1

Remarques :

- si le référentiel (1) de mise à jour et de consultation est indisponible, il ne sera plus possible de mettre à jour l'annuaire ENT, que ce soit automatiquement ou via l'IHM de gestion de contenu ;
- si les référentiels (1) et (2) sont indisponibles en même temps, toutes les requêtes seront redirigées sur le même référentiel (1') de secours, avec un risque de dégradation des performances.

5.2. Architecture – option 2

L'option 2 (Figure 16) complète l'option 1. La redirection des requêtes par un proxy LDAP (ou un commutateur niveau 7) est reprise. Cependant, cette option permet en plus d'assurer la haute-disponibilité pour les actes de mises à jour et de gestion via l'IHM de gestion de contenu.

L'IHM de gestion de contenu est redondée et les requêtes correspondantes passent désormais par le proxy LDAP (ou commutateur niveau 7). En fonctionnement nominal, ces requêtes sont dirigées vers le référentiel (1) de mise à jour et de consultation. Si celui-ci n'est pas disponible, elles sont alors redirigées vers le référentiel (1') de secours.

Afin que les modifications apportées au référentiel (1') de secours lors d'un dysfonctionnement soient prises en compte dans le référentiel (1), une réplication totale multi-maîtres est mise en place entre les référentiels (1) et (1').

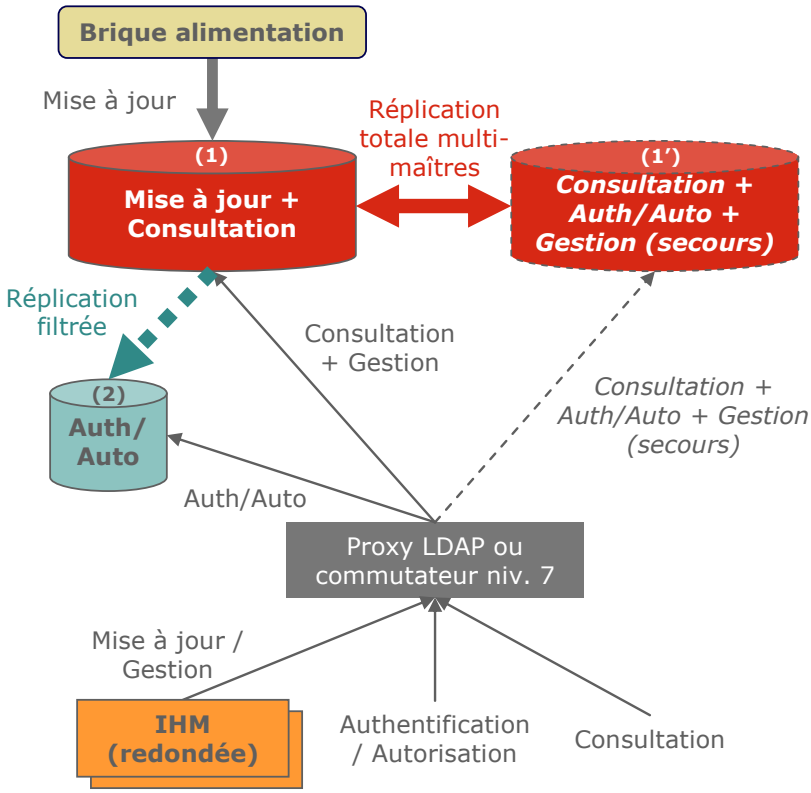

Figure 16 : Architecture – Option 2

Remarques :

Si le référentiel (1) de mise à jour et de consultation est indisponible, il ne sera plus possible de mettre à jour l'annuaire ENT via la brique d'alimentation.

Les modifications apportées au référentiel (1') lors d'un fonctionnement en mode secouru ne seront répercutées sur le référentiel (2) d'authentification / autorisation que lorsque le référentiel (1) sera de nouveau opérationnel.

5.3. Architecture – option 3

L'option 3 (Figure 17) généralise la haute-disponibilité à tous les composants de l'architecture et ajoute la répartition de charge. Elle est constituée des éléments suivants :

- deux référentiels de mise à jour, consultation et gestion : (1) et (1'), une réplication totale multi-maîtres étant mise en place entre ces deux référentiels ;
- deux référentiels d'authentification / autorisation : (2) et (2'), une réplication totale multi-maîtres étant mise en place entre ces deux référentiels ; ils sont alimentés par réplication filtrée, respectivement depuis les référentiels (1) et (1') ;
- un commutateur niveau 7, secouru en *Heartbeat*, répartissant les requêtes de mise à jour / gestion, d'authentification / autorisation et de consultation sur deux proxy LDAP en fonction de leur charge ;
- chaque proxy LDAP n'est relié qu'à un seul référentiel de mise à jour, consultation et gestion ((1) ou (1')) et un seul référentiel d'authentification / autorisation ((2) ou (2')) ; le proxy redirige alors les requêtes vers le référentiel adéquat.

Les applications et l'IHM de gestion de contenu ne s'adressent qu'au commutateur.

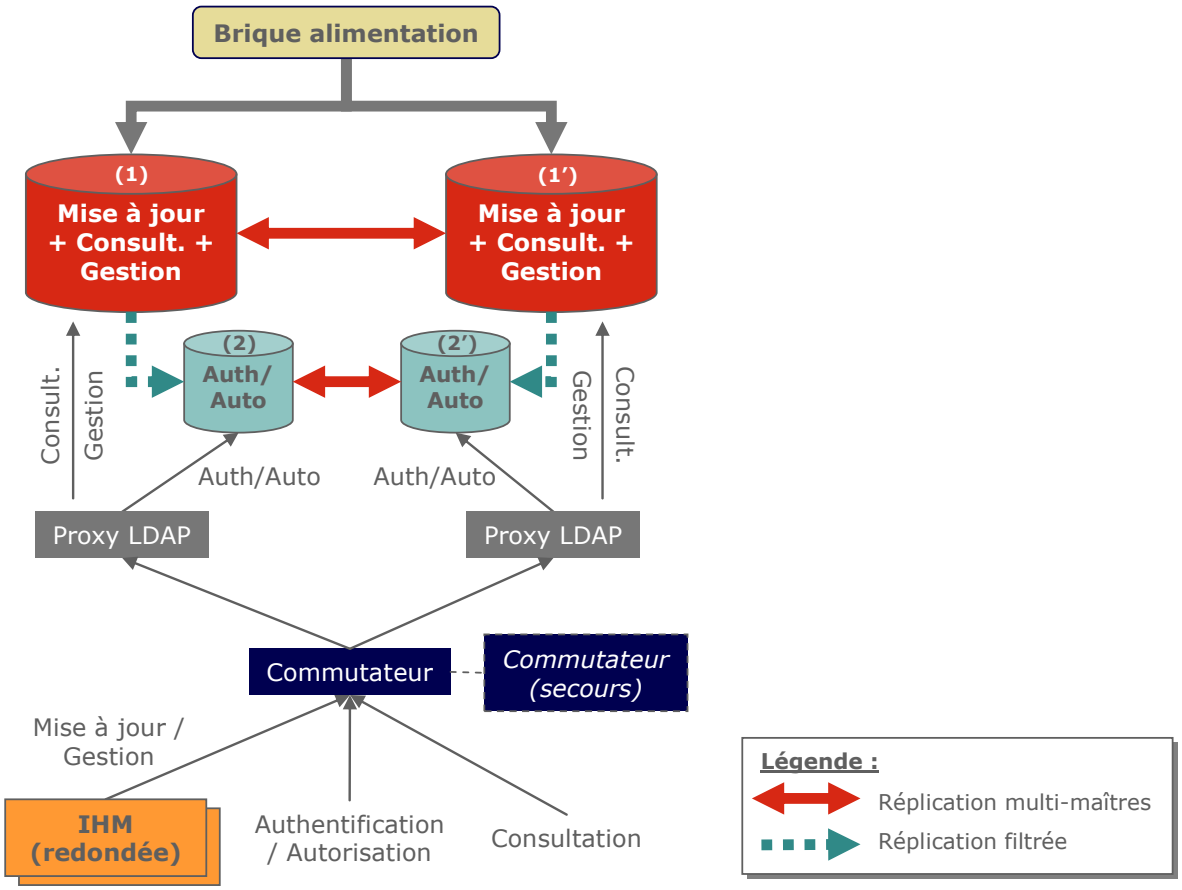

Figure 17 : Architecture – Option 3

Remarque : Cette architecture pourrait permettre de localiser sur deux sites différents les référentiels (1)–(2) et (1')–(2').

6. Services de l'annuaire ENT

Cette partie décrit l'ensemble des services attendus pour l'annuaire ENT.

Le soumissionnaire détaillera, pour chaque fonctionnalité, le mode de fonctionnement de sa solution et les principes de mise en œuvre (prérequis, développements et paramétrages nécessaires…). Une distinction claire devra être effectuée entre les fonctionnalités natives (ne nécessitant qu'un paramétrage), les fonctionnalités à développer, et les fonctionnalités non prises en charge.

La maîtrise d'ouvrage en charge du projet ENT pourra, en fonction de ses besoins, ne pas faire figurer dans son cahier des charges certaines fonctionnalités présentées ci-après, ou a contrario ajouter certaines fonctionnalités manquantes.

Par ailleurs, elle précisera les éléments suivants : charte graphique et gabarit des IHM, cinématique et dynamique des pages.

6.1. Services de gestion

6.1.1. Services d'alimentation

[SRV-1] Alimentation depuis un fichier

Deux types d'alimentation par fichiers sont envisageables :

- alimentation depuis un fichier XML fourni par le MEN ou le ministère en charge de l'Agriculture ; le fichier XML fourni par le MEN ou le ministère en charge de l'Agriculture comporte les objets personnes et structures gérés respectivement par le MEN ou le ministère en charge de l'Agriculture ainsi que leurs caractéristiques ; le format de ce fichier est détaillé à l'annexe 4 ;
- alimentation depuis un fichier fourni par une autre source externe ; le soumissionnaire proposera a minima un connecteur permettant l'alimentation de l'annuaire ENT à partir de fichiers plats.

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement compléter ce chapitre avec les informations concernant les autres sources d'alimentation (par exemple SI de la collectivité locale ou SI du ministère en charge de l'Agriculture). Les fichiers en question pourront être de type XML, DSML, CSV, LDIF, etc.

Les services d'alimentation doivent :

- permettre de créer, modifier, et supprimer des personnes et des structures, et leurs attributs dans l'annuaire ENT, à partir des données fournies dans le fichier plat, en définissant des règles de synchronisation et de jointure ;
- permettre de définir les fréquences d'alimentation ;
- permettre de suspendre une alimentation à tout moment ;
- implémenter des mécanismes de contrôle du format des fichiers en entrée, de gestion des erreurs (reprises), de gestion des doublons, de vérification des règles de synchronisation, de vérification des contraintes d'intégrité définies au chapitre 3.3 ; les contraintes d'intégrité liées à une limite quantitative (exemple : nombre maximum d'élèves délégués par classe) devront être paramétrables ;
- implémenter des notifications d'alertes en cas d'erreur ou de non-respect de règles ou de contraintes ; ces alertes pourront être classées en différents niveaux. Selon le niveau d'alerte, le mécanisme d'alimentation pourra ou non être stoppé.

La maîtrise d'ouvrage en charge du projet ENT pourra préciser les niveaux d'alertes et les processus associés qu'elle souhaite mettre en œuvre, ou laisser à la discrétion du soumissionnaire le fait d'effectuer des propositions en ce sens.

Remarque : L'alimentation des mots de passe ne fait pas partie des fonctions attendues pour les services d'alimentation.

[SRV-2] Règles de gestion de l'alimentation

Les services d'alimentation doivent prendre en compte des règles de gestion de l'alimentation, et nomment :

- des règles de transformation de la casse des attributs alimentés ;
- des règles de construction des clés de jointure (cf. chapitre 4.4.7) ;
- des règles de répartition des objets alimentés entre les différentes catégories de personnes et de structures gérées au sein de l'annuaire ENT ;
- des règles de transformation des références (entre objets alimentés) en *dn* pointant vers des objets de l'annuaire ENT.

Les règles de gestion pourront être **spécifiques à chaque source autoritaire**. Les règles concernant l'alimentation depuis le SI du MEN ou du ministère en charge de l'Agriculture sont décrites à l'annexe 4.

La maîtrise d'ouvrage en charge du projet ENT pourra compléter ce chapitre avec des règles de gestion complémentaires, notamment par rapport à d'autres sources d'alimentation que le SI du MEN ou le SI du ministère en charge de l'Agriculture.

[SRV-3] Réconciliation de comptes utilisateurs

Les informations concernant une même personne physique peuvent provenir de différentes sources autoritaires, notamment lorsqu'une personne appartient à plusieurs catégories de personnes. Ainsi, les informations d'un parent d'élève travaillant pour une collectivité locale proviendront à la fois du SI du MEN et du SI de la collectivité.

Par ailleurs, pour une même source autoritaire, une même personne physique peut être vue comme deux objets différents, et donc être alimentée sous deux clés de jointure différentes, notamment lorsqu'un parent d'élève reçoit un compte associé à chacun de ses enfants identifiés dans l'ENT. Une réconciliation sera donc nécessaire également dans ce cas (cf. annexe 4 pour l'alimentation depuis le SI du MEN.

Deux types de réconciliation sont identifiés :

- le rapprochement de comptes : cette opération réconcilie deux comptes institutionnels de sources autoritaires différentes ou de deux comptes séparés d'une même source autoritaire. Les deux comptes restent actifs mais un seul, le compte principal, est utilisé pour accéder à l'ENT. L'autre compte, le compte principal, reste présent pour intégrer les mises à jour qui le concernent (au niveau de son entrée LDAP et de ses appartenances dans les groupes), venant des différentes sources autoritaires ;
- la fusion de comptes : cette opération intègre les informations venant d'un compte manuel temporaire dans un compte institutionnel. Une fois la fusion effectuée, le compte manuel est archivé.

Le service de réconciliation doit notamment contrôler l'exclusivité de la relation d'un compte identifié comme secondaire avec un compte principal. Autrement dit, un compte secondaire déjà réconcilié ne peut plus être rapproché avec un autre compte, tant que la relation de réconciliation existante est active, et tant que le compte principal est référencé au niveau de l'annuaire de l'ENT.

Afin que chaque personne physique puisse disposer d'un seul compte sur l'annuaire ENT (et donc d'un seul identifiant de connexion), les services d'alimentation doivent permettre de réconcilier les informations issues des différentes sources autoritaires. Cette réconciliation ne pourra se faire qu'à l'initiative de la personne concernée ou de l'administrateur de l'ENT.

Pour tout objet « Personne », le principe de réconciliation est le suivant :

- la personne se connecte à l'ENT à l'aide d'un de ses comptes, <compte1>, puis accède au service de réconciliation ;
- l'ENT demande à la personne :
  - de saisir à nouveau le mot de passe de <compte1>,
  - de saisir l'identifiant de connexion (login) et le mot de passe du ou des comptes qui doivent être réconciliés avec <compte1>,
  - de choisir le compte de référence parmi <compte1> et les autres comptes. Ce compte de référence détermine :
    - l'identifiant de connexion et le mot de passe qui seront utilisés pour les prochains accès à l'ENT,
    - les informations qui seront conservées en cas de divergence entre les différentes sources (nom de famille orthographié différemment par exemple) ;
- après vérification des identifiants de connexion et des mots de passe, l'ENT :
  - ajoute les informations provenant des différents comptes au compte de référence,
  - conserve l'ensemble des clés de jointure,
  - rappelle à la personne l'unique identifiant de connexion qui doit désormais être utilisé.

Au niveau de l'annuaire de l'ENT, le principe de réconciliation est le suivant :

- l'administrateur se connecte à l'ENT, puis accède au service de réconciliation ;
- l'ENT demande à l'administrateur :
  - de saisir l'identifiant de connexion (login) du <compte1>,
  - de saisir l'identifiant de connexion (login) du ou des comptes qui doivent être réconciliés avec <compte1>,
  - de choisir le compte de référence parmi <compte1> et les autres comptes. Ce compte de référence détermine :
    - l'identifiant de connexion et le mot de passe qui seront utilisés pour les prochains accès à l'ENT,
    - les informations qui seront conservées en cas de divergence entre les différentes sources (nom de famille orthographié différemment par exemple) ;
- après vérification des identifiants de connexion, l'ENT :
  - ajoute les informations provenant des différents comptes au compte de référence,
  - conserve l'ensemble des clés de jointure,
  - notifie à la personne concernée l'unique identifiant de connexion qui doit désormais être utilisé.

Remarque : dans le cadre d'une fédération d'identités, même si l'opération de réconciliation est effectuée au niveau de l'outil de gestion des identités, cette réconciliation doit être répercutée vers l'annuaire ENT afin de mutualiser les informations des deux comptes au sein de l'ENT.

La maîtrise d'ouvrage en charge du projet ENT pourra préciser et détailler le modèle retenu pour la prise en compte des demandes de réconciliation (modèle synchrone ou modèle asynchrone), ainsi que les services mis en œuvre pour mutualiser les données venant des deux comptes rapprochés ou pour migrer les données du compte source vers le compte cible lors d'une fusion.

6.1.2. Services de gestion de contenu

[SRV-4] Environnement de gestion central et unique

Le service de gestion de contenu doit proposer un environnement de gestion central et unique donnant accès aux fonctions de gestion des entrées de l'annuaire ENT.

L'accès à l'environnement de gestion des entrées est réservé aux administrateurs centraux et locaux, et aux utilisateurs. Ils doivent se signer par la fourniture d'un couple « identifiant / mot de passe ».

[SRV-5] Gestion des personnes et des structures

Le service de gestion de contenu doit permettre d'appliquer des opérations (création, modification, suppression) sur les personnes et les structures de l'annuaire ENT :

- gestion des d'entrées correspondant à des personnes :
  - Création / suppression d'entrées,
  - Modification des attributs d'une entrée,
  - Ajout / suppression d'une catégorie à une personne ;
- gestion des d'entrées correspondant à des structures :
  - Création / suppression d'entrées,
  - Modification des attributs d'une entrée.

Le service de gestion de contenu doit notamment contrôler les contraintes d'intégrité mentionnées au chapitre 3.3 et permettre de gérer les multiples relations d'un élève avec des personnes en relation avec les élèves.

Ces différentes opérations seront par ailleurs implémentées en conformité avec les contraintes d'intégrité présentées aux chapitres 3.3 et 4.2.1.

Remarques :

- ces fonctions seront notamment utilisées pour compléter le peuplement de l'annuaire ENT avec les catégories de personnes et de structures qui ne sont pas alimentées automatiquement ;
- toute donnée issue de l'alimentation du MEN ou du ministère en charge de l'Agriculture n'est pas modifiable dans l'interface de gestion de contenu, à l'exception de certains attributs mentionnés dans la colonne « Alimentation » du tableau de l'annexe 2. Ces attributs sont en effet initialisés par l'alimentation MEN ou ministère en charge de l'Agriculture puis proposés en self-service (civilité pour les élèves par exemple).

[SRV-6] Gestion des nomenclatures

Le service de gestion de contenu doit offrir une fonction de gestion des nomenclatures. Ce service consiste en l'implémentation et en la gestion d'une table de nomenclature locale permettant d'associer chaque attribut ne disposant pas d'une nomenclature nationale à une nomenclature définie localement.

[SRV-7] Gestion des listes rouges

L'outil de gestion de contenu doit permettre de gérer des listes rouges d'utilisateurs.

Ces utilisateurs n'apparaîtront pas dans les pages blanches. Les informations sur ces utilisateurs serviront uniquement à déterminer leurs habilitations.

Remarque : Cette fonctionnalité sera notamment utilisée dans le cas d'élèves placés sous protection juridique.

[SRV-8] Gestion des groupes de personnes / groupes de structures

Cette fonction offre la possibilité de gérer des groupes de personnes (classes, groupes de langue…) et des groupes de structures (regroupement d'établissements…).

- création / suppression d'entrées ;
- modification de la liste des membres (ajout / suppression de membres).

Ces groupes peuvent être peuplés de trois manières :

- « Discrétionnaire » : le groupe est peuplé / dépeuplé manuellement par l'administrateur ;
- « Automatique » : le groupe est peuplé / dépeuplé automatiquement en fonction de règles de peuplement basées sur des combinaisons de valeurs des attributs des personnes ou structures ;
- « Mixte » : à la fois discrétionnaire et automatique.

Il est également possible de créer des groupes de groupes. Les objets peuplés peuvent être des groupes ou des personnes (ou structures). Le nombre de récursivité n'est pas limité.

[SRV-9] Gestion des profils applicatifs

Cette fonction offre la possibilité de gérer des profils applicatifs.

- création / suppression ;
- modification de la liste des membres (ajout / suppression de membres).

Ces profils peuvent être peuplés de trois manières :

- « Discrétionnaire » : le profil applicatif est peuplé / dépeuplé manuellement par l'administrateur ;
- « Automatique » : le profil applicatif est peuplé / dépeuplé automatiquement en fonction de règles de peuplement basées sur des combinaisons de valeurs des attributs des personnes ;
- « Mixte » : à la fois discrétionnaire et automatique.

Il est également possible de créer des profils applicatifs de profils applicatifs. Les objets peuplés peuvent être des groupes ou des personnes. Le nombre de récursivité n'est pas limité.

Un profil applicatif peut être exclusif. Une personne associée à un profil applicatif exclusif ne peut être associée à tout autre profil applicatif ou à certains profils applicatifs.

Un profil peut hériter d'un profil applicatif existant. L'ensemble des attributs du profil applicatif hérité est alors associé automatiquement au profil applicatif héritant, dont notamment la liste des personnes membres du profil applicatif et les rôles applicatifs associés.

[SRV-10] Gestion des rôles applicatifs

Cette fonction offre la possibilité de gérer des rôles applicatifs.

- création / suppression ;
- association à une ou plusieurs applications ;
- gestion de l'association à un ou plusieurs profils applicatifs.

Remarque : Une personne peut directement être associée à un rôle applicatif, soit de manière discrétionnaire, soit de manière automatique, sans l'intermédiaire d'un profil applicatif associé à ce rôle.

[SRV-11] Gestion des applications

Sur son périmètre d'administration, un administrateur peut créer, modifier, supprimer une application.

Une application peut être associée à zéro, un, ou plusieurs rôles applicatifs.

Remarque : Certains éléments caractérisant les applications sont liés aux services AAS implémentés, et ne sont pas intégrés à ce document (exemples : période d'accès, typologie d'accès, modes d'authentification...).

[SRV-12] Délégation des droits d'accès aux données de l'annuaire ENT

Des droits d'accès en lecture / écriture sont positionnés sur les objets et attributs de l'annuaire ENT.

Des périmètres distincts d'administration sont définis pour chaque administrateur (délégation ou répartition de l'administration des utilisateurs).

Les périmètres suivants peuvent être définis :

- des portées d'administration : objets et attributs de ces objets ;
- des actions d'administration sur ces portées :
  - droits : lecture, création, modification, suppression de données,
  - capacité à déléguer ces droits :
    - à une ou plusieurs personnes (de manière discrétionnaire, par appartenance à un groupe…),
    - sur une période donnée (date d'effet / date de fin),
    - attribution de tout ou partie des droits dont on dispose,
    - attribution de la capacité de déléguer tout ou partie de ces droits à d'autres personnes.

Des recouvrements de périmètres entre administrateurs sont possibles.

Un niveau hiérarchique est associé à chaque administrateur. Un administrateur de niveau *n* peut annuler toutes les actions réalisées par les administrateurs de niveau inférieur ou modifier toutes les données accessibles par les administrateurs de niveau inférieur.

Un administrateur peut ainsi définir les droits d'un utilisateur sur les attributs le caractérisant (lecture / écriture / capacité de délégation d'administration sur ses attributs).

Exemple d'implémentation : définitions

Ces différents services permettent par exemple de décliner l'organisation suivante, selon quatre niveaux : administrateur central, propriétaire, gestionnaire, utilisateur.

1) *l'administrateur central a en charge la création et la gestion des objets transverses à l'ENT tels que les profils applicatifs partagés, et les rôles applicatifs et les applications transverses ;*
2) *les propriétaires possèdent les droits en écriture sur les objets de leur périmètre, et définissent pour chacun des attributs d'un type d'objet :*
   - *les gestionnaires et leurs droits (lecture / écriture),*
   - *la capacité à déléguer ces droits ;*
3) *les gestionnaires sont responsables de la gestion / mise à jour des objets / attributs ;*
4) *un utilisateur est un gestionnaire particulier, n'ayant des droits d'écriture et de capacité à déléguer un droit en lecture ou en écriture uniquement sur ses attributs.*

Notons que la maîtrise d'ouvrage en charge du projet ENT doit présenter au chapitre 8.1 l'organisation retenue dans le cadre de son projet ENT.

Remarque : Au regard du schéma d'annuaire (cf. chapitre 4.2) et de l'organisation de la gestion du contenu envisagée (cf. chapitre 8.2), le soumissionnaire précisera s'il est envisageable de positionner des ACL[14] de premier niveau directement sur l'annuaire, ou si l'ensemble de ces droits devra être géré au niveau des services de gestion de contenu. Dans le premier cas, il précisera quelles ACL doivent être positionnées.

[14] ACL : Access control list (liste de contrôle d'accès)

[SRV-13] Délégation des droits d'accès sur les applications

Une personne, sous réserve qu'elle soit autorisée à le faire, doit pouvoir déléguer tout ou partie de ses droits d'accès à une ou plusieurs applications, et ce de manière temporaire.

Une délégation temporaire de droits se caractérise par :

- une liste de personnes à qui les droits (tout ou partie des droits possédés) sont délégués (liste discrétionnaire, liste basée sur un groupe de personnes ou sur un profil applicatif). ;
- une période donnée : une date d'effet et une date de fin de cette délégation pour chaque personne déléguée ;
- la capacité pour chaque personne déléguée de déléguer elle-même à d'autres personnes tout ou partie de ces droits.

[SRV-14] Gestion des suspensions

Le service de gestion offre la capacité de suspendre les personnes.

Lorsqu'une personne est suspendue, toutes ses caractéristiques sont conservées (attributs, liens…) mais la personne ne peut pas accéder aux applications de l'ENT.

Il est également possible de positionner pour toute personne une date d'activation et une date de fin de validité. En fonction de ces dates, des traitements de suspension ou de notification de suspension peuvent être lancés.

Il est possible de réactiver une personne suspendue.

[SRV-15] Import / export de fichiers

Le service de gestion de contenu doit permettre :

- d'importer un fichier afin de peupler l'annuaire ENT ;
- d'exporter dans un fichier des entrées sélectionnées.

Les formats de fichier devant être pris en charge sont les suivants : CSV, LDIF, XML.

[SRV-16] Outil de *workflow*

Les processus définis au chapitre 8.2 doivent être informatisés. Pour ce faire, les fonctions de *workflow* suivantes sont attendues :

- une interface graphique et simple d'utilisation permettant de créer et de gérer les *workflows* relatifs aux processus de l'ENT ;
- la capacité à gérer les fonctionnalités classiques de *workflow* : validation en série, en parallèle, escalade en cas de non traitement dans les délais impartis, champs à renseigner de façon obligatoire ou facultative pour valider une étape du *workflow*, envoi de notification par mail, envoi de mail prédéfini selon la ressource traitée, édition d'état papier…

[SRV-17] Changement de mot de passe

Le service de gestion de contenu doit permettre aux utilisateurs de modifier leur mot de passe. Cette action nécessite :

- de saisir l'ancien mot de passe ;
- de saisir et confirmer le nouveau mot de passe.

Les mots de passe ne doivent pas être stockés en clair. Ils devraient être stockés de manière chiffrée et irréversible, éventuellement sous forme d'empreintes numériques (cf. document [2]).

[SRV-18] Création / modification / suppression de l'alias

La maîtrise d'ouvrage en charge du projet ENT pourra supprimer cette fonctionnalité s'il ne souhaite pas la proposer.

Un utilisateur peut se créer, s'il le souhaite, un alias de connexion l'ENT. Il ne peut disposer que d'un seul alias. La règle retenue pour la création des alias sur le périmètre de l'ENT est la suivante : « premier arrivé, premier servi ».

La maîtrise d'ouvrage en charge du projet ENT pourra envisager de demander au soumissionnaire la mise en œuvre d'un workflow *spécifique de validation des demandes d'alias afin d'empêcher l'utilisation de noms d'alias réservés, vulgaires, pouvant induire en erreur…*

[SRV-19] Demande de modification de ses propres informations

Le service de gestion de contenu doit permettre à une personne de demander des modifications sur certains de ses attributs non accessibles en écriture : changement de coordonnées, erreur de saisie… via l'utilisation d'un *workflow*.

La fiche de l'utilisateur passe alors en mode « édition ». Les modifications ne sont pas inscrites dans l'annuaire ENT mais transmises à la personne définie dans le *workflow*.

6.2. Services d'accès

6.2.1. Services de sécurité

Ce chapitre présente les services de sécurité utilisés par les services AAS.

En fonction des services AAS retenus, la maîtrise d'ouvrage en charge du projet ENT pourra étendre la couverture fonctionnelle de ces services. En effet, seuls les services fondamentaux d'authentification et d'autorisation sont demandés par la suite.

Au regard des services demandés, le soumissionnaire indiquera les extensions de schéma LDAP nécessaires et les éventuels impacts sur l'architecture technique.

[SRV-20] Gestion de l'authentification

Lors de l'accès d'une personne à une application de l'ENT, les services AAS vérifient au travers d'une requête d'authentification la validité du couple « identifiant de connexion / mot de passe » dans l'annuaire ENT.

- paramètres d'entrée : identifiant de connexion / mot de passe ;
- paramètres de sortie : OK / NOK.

Remarque : L'utilisation d'un alias de connexion est possible.

La maîtrise d'ouvrage en charge du projet ENT pourra supprimer cette remarque s'il ne souhaite pas proposer la fonctionnalité d'alias.

[SRV-21] Gestion du multi-rôles

La maîtrise d'ouvrage en charge du projet ENT pourra supprimer cette fonctionnalité s'il ne souhaite pas la proposer.

Une personne, lorsqu'elle souhaite accéder à une application pour laquelle elle possède plusieurs « rôles », peut choisir, lors de la phase d'authentification, avec quel rôle elle se connecte. Elle retrouve alors uniquement l'environnement applicatif et les droits associés au rôle choisi.

Remarque : Cette fonction peut nécessiter l'utilisation du service de réconciliation de comptes.

[SRV-22] Gestion de l'autorisation

Lors de l'accès d'une personne à une application de l'ENT, les services AAS vérifie au travers d'une requête d'autorisation si la personne est autorisée à accéder à l'application demandée.

Le contrôle d'autorisation sur une application peut être réalisé sur la valeur d'un attribut de la personne, sur l'appartenance de la personne à un profil applicatif, sur l'appartenance de la personne à un rôle applicatif. Il ne peut se baser que sur un sous-ensemble défini des objets et attributs de l'annuaire ENT. Cette liste est précisée en annexe 2.

Aussi, plusieurs types de requête sont envisageables :

- Requête autorisation de type 1 :
  - paramètres d'entrée : identifiant de connexion de la personne / identifiant d'attribut / valeur d'attribut ;
  - paramètres de sortie : OK / NOK.
- Requête autorisation de type 2 :
  - paramètres d'entrée : identifiant de connexion de la personne / identifiant de profil applicatif ;
  - paramètres de sortie : OK / NOK.
- Requête autorisation de type 3 :
  - paramètres d'entrée : identifiant de connexion de la personne / identifiant de rôle applicatif ;
  - paramètres de sortie : OK / NOK.
- Requête autorisation de type 4 :
  - paramètres d'entrée : identifiant de connexion de la personne ;
  - paramètres de sortie : liste des profils applicatifs associés à la personne.
- Requête autorisation de type 5 :
  - paramètres d'entrée : identifiant de connexion de la personne ;
  - paramètres de sortie : liste des rôles applicatifs associés à la personne.

6.2.2. Services de publication

[SRV-23] Publication pour les applications

Les applications de l'ENT, en cohérence avec leurs droits d'accès aux données de l'annuaire ENT, peuvent interroger l'annuaire ENT pour récupérer tout ou partie des caractéristiques d'une personne, d'une structure, la liste des membres d'un profil applicatif…

[SRV-24] Pages Blanches

Une personne peut consulter les fiches des autres personnes de l'ENT. Ces fiches pourraient comporter les zones suivantes afin d'organiser les informations :

- informations civiles ;
- coordonnées personnelles ;
- coordonnées professionnelles ;
- informations administratives ;

- scolarité ;
- divers.

En fonction de ses droits, une personne ne pourra consulter que certaines informations sur les fiches des autres personnes.

Lorsque les attributs des fiches font référence à des entrées de l'annuaire ENT (des personnes, des structures, des classes, des groupes…), des liens hypertextes doivent permettent d'accéder aux fiches correspondant à ces entrées.

[SRV-25] Pages Jaunes

Une personne peut consulter les fiches des structures gérées par l'ENT. Ces fiches pourraient comporter les zones suivantes afin d'organiser les informations :

- informations légales ;
- coordonnées géographiques ;
- coordonnées du standard ;
- divers.

Remarque : Toutes les informations des fiches des structures sont consultables librement par toutes les personnes de l'ENT.

La maîtrise d'ouvrage en charge du projet ENT pourra éventuellement amender la remarque ci-dessus.

Le service de consultation doit également permettre d'accéder aux fiches correspondant aux différents groupes de l'annuaire ENT (classes, groupes, regroupements d'établissements…) afin d'obtenir la liste des membres de ces groupes.

[SRV-26] Navigation

Les Pages Blanches doivent proposer une navigation arborescente avec affichage sur la zone principale de l'IHM de la fiche sélectionnée. Les arborescences suivantes doivent être proposées a minima :

- par établissement, puis par catégorie de personnes, puis par ordre alphabétique ;
- pour un établissement, par catégorie de personnes, puis par ordre alphabétique ;
- par structure (établissement, services académiques, collectivité locale), puis par catégorie de personnes (consolidation).

[SRV-27] Recherche

La recherche constitue une fonctionnalité particulièrement importante du service de gestion de contenu. Ce dernier doit en effet permettre à la fois une recherche très ciblée et une recherche beaucoup plus générale.

Les recherches peuvent porter sur les différents attributs des catégories de personnes et notamment le nom, le prénom, la structure de rattachement, le niveau scolaire…

Pour les attributs dont la nomenclature définit une liste fermée, l'interface doit proposer des listes de choix en plus d'un champ libre.

L'outil doit permettre l'utilisation d'expressions logiques pour constituer des requêtes de recherche.

Des requêtes « standard » doivent également être proposées aux utilisateurs. La liste ci-dessous donne quelques exemples de requêtes qui pourraient être proposées :

- rechercher toutes les personnes de la catégorie <*liste de catégories*> dans l'établissement <*liste d'établissements*> ;

- rechercher toutes les personnes de la catégorie <*liste de catégories*> liées à la classe/groupe <*liste des classes/groupes*> ;
- rechercher tous les <*catégorie de personnes*> dans l'établissement <*liste d'établissements*> ;
- rechercher tous les enseignants [respectivement les élèves] qui enseignent [respectivement qui suivent] l'enseignement <*liste d'enseignements*> ;
- rechercher toutes les personnes qui exercent la fonction ou le domaine <*liste de fonctions/domaines*>.

Le résultat de la recherche doit être présenté sous forme de tableau ou de liste. Un lien doit permettre de consulter la fiche correspondant à chacune des entrées retournées en résultat de la recherche.

La notion de « panier » doit être implémentée par l'outil de gestion de contenu. Ce terme désigne la capacité à conserver des entrées du résultat d'une requête pour effectuer des actions postérieures (exemples : envoi d'e-mail ou impression de chacune des fiches correspondantes…).

[SRV-28] Édition

Il est possible d'exporter une fiche, le résultat d'une recherche ou toutes les fiches issues d'une recherche dans un fichier, en précisant notamment :

- les fiches à exporter par rapport au résultat d'une recherche (quelles personnes, quelles structures) ;
- les attributs à exporter pour chaque fiche.

Les formats de fichier devant être pris en charge sont les suivants : PDF, CSV.

[SRV-29] Impression

Une fiche « Personne », une fiche « Structure », le résultat d'une recherche ou toutes les fiches issues d'une recherche peuvent être imprimées.

6.3. Services techniques

[SRV-30] Gestion des traces et historisation

Toute action ou activité doit être tracée et stockée dans des journaux, et en particulier :

- flux d'alimentation de l'annuaire :
  - type de flux,
  - date de début et date de fin de l'accès,
  - actes de gestion réalisés : actions, données ;
- accès des utilisateurs avec leur compte :
  - identifiant de la personne,
  - date de début et date de fin de l'accès,
  - identifiant des applications accédées, durée de connexion par application ;
- actions de gestion des administrateurs :
  - identifiant de la personne,
  - date de début et date de fin de l'accès,
  - actes de gestion réalisés : actions, données,
- accès aux journaux et actions sur les journaux :
  - identifiant du compte,

- date de début et date de fin de l'accès,
- actes réalisés : actions, données ;

- tentatives d'accès infructueuses :
  - identifiant de la personne,
  - date,
  - motifs de l'échec.

[SRV-31] Journaux d'accès

L'accès aux journaux est soumis à une authentification et un contrôle d'autorisation. Les administrateurs habilités doivent se signer par la fourniture d'un couple « identifiant de connexion / mot de passe ».

Le système offre une fonction de gestion des journaux permettant d'archiver les journaux, de les visualiser, de réaliser des tris sur la base de toutes les informations qu'ils contiennent (identifiant de personne, applications accédées…), de les éditer ou de réaliser des exports.

Chaque administrateur habilité doit avoir la possibilité de se créer ses propres fonctions de tris en choisissant les critères et le format de représentation des résultats. Des fonctions de recherche mono-critère ou multi-critères sur les informations contenues dans les journaux sont mises à la disposition des administrateurs.

[SRV-32] Audit et reporting

Le service d'audit et reporting doit fournir une vision centralisée des habilitations des utilisateurs au travers de tableaux de synthèse. Ces tableaux doivent notamment présenter les informations suivantes :

- utilisateurs appartenant à un profil applicatifs ou à un rôle applicatif ; profils applicatifs et rôles applicatifs d'un utilisateur ;
- rôles applicatifs associés à un profil applicatif ; profils applicatifs associés à un rôle applicatif ;
- applications utilisant un profil applicatif ou un rôle applicatif ; rôles applicatifs et profils applicatifs utilisés par une application ;
- personnes accédant à une application.

[SRV-33] Supervision

La solution mettra en œuvre des fonctionnalités permettant la détection automatique des erreurs de fonctionnement de la solution. Ces erreurs seront alors tracées automatiquement, la localisation du fichier de trace pouvant être paramétrée.

Le soumissionnaire précisera les outils de supervision supportés par sa solution, les modalités de cette compatibilité et la typologie des incidents pouvant être générés, par composant.

[SRV-34] Administration et pilotage

La solution mettra en œuvre une administration technique centralisée de la solution.

Le soumissionnaire détaillera les moyens mis en œuvre pour cette administration et, si la solution nécessite d'ordonnancer certains travaux, détaillera les outils d'ordonnancement supportés par la solution proposée.

[SRV-35] Sauvegarde / archivage

La solution mettra en œuvre des fonctionnalités de sauvegarde. Ces fonctionnalités permettront :

- des sauvegardes à intervalle régulier paramétrable et cela sans arrêt du service ;

- des restaurations déclenchées manuellement et cela sans arrêt du service.

Ce service devra également offrir des fonctions paramétrables d'archivage des données.

Le soumissionnaire précisera sur la base de son expérience l'ensemble des données à sauvegarder par composant de la solution, et les outils de sauvegarde supportés par sa solution et les modalités de cette compatibilité.

6.4. API de service

[SRV-36] API de service

L'ensemble des services présentés précédemment doivent être accessibles via des API développées en C ou JAVA.

[SRV-37] Couche de services

En option, le soumissionnaire pourra proposer la réalisation d'une couche de services permettant de rendre les applications indépendantes du modèle de données de l'annuaire ENT, limitant ainsi les impacts en cas d'évolution de celui-ci.

Il devra choisir une méthode d'implémentation de la couche de services (de préférence basée sur une architecture « Web Services » à l'aide des techniques SOAP / WSDL / UDDI) et fournir un schéma d'architecture technique expliquant la mise en place de cette couche de services.

7. Exigences sur l'annuaire ENT

[EX-1] Volumétrie

Le volume des données stockées dans l'annuaire ENT est un élément structurant pour la définition de l'architecture technique. Ainsi, la maîtrise d'ouvrage en charge du projet ENT indiquera précisément, pour les années à venir, le périmètre couvert par le projet ENT afin que le soumissionnaire puisse établir une réponse argumentée du dimensionnement de sa solution : nombre d'élèves concernés par le projet, nombre d'établissements concernés par le projet, etc.

Les éléments de volumétrie et les hypothèses d'accès donnés dans ce chapitre peuvent permettre au soumissionnaire de déterminer l'option d'intégration des exigences de disponibilité et de la répartition de charge la plus adaptée pour respecter les temps de réponse exigés pour l'ENT.

À titre d'illustration, les hypothèses suivantes peuvent être considérées :

- Pour 100 élèves, on compte :
  - 125 responsables d'élèves ;
  - 10 enseignants ;
  - 5 non enseignants.
- Les autres catégories de personnes représentent une quantité non significative.

Pour 1 élève inscrit dans l'ENT, il y a donc environ (100 + 125 + 10 + 5) / 100 = **2,4 personnes**.

[EX-2] Intégration dans l'existant

La solution proposée devra s'intégrer, autant que faire se peut, sans interférence avec l'existant technique (supervision, sauvegarde, exploitation…).

La maîtrise d'ouvrage en charge du projet ENT précisera cet existant technique ou fera référence à sa description réalisée dans le SDET.

[EX-3] Référentiel technique

La solution proposée devra être conforme au référentiel technique en termes de systèmes et de plate-forme utilisés.

La maîtrise d'ouvrage en charge du projet ENT précisera ce référentiel technique ou fera référence à sa description réalisée dans le SDET.

[EX-4] Performances sur les requêtes des services de sécurité

Le niveau de qualité de service exigé est plus élevé pour le référentiel d'authentification / autorisation. L'objectif est donc de s'assurer que les requêtes sur ce référentiel pourront être traitées dans les temps.

La maîtrise d'ouvrage en charge du projet ENT pourra les compléter ou les modifier au vu de son expérience.

Les hypothèses sur la période chargée sont les suivantes :

- environ 25% de la population d'un établissement d'enseignement est amenée à se connecter à l'ENT. Les catégories de personnes concernées sont les élèves, les enseignants, les non enseignants rattachés administrativement aux services académiques, les non enseignants rattachés administrativement à une collectivité locale, les non enseignants rattaché administrativement à un établissement et les personnels extérieurs ;

- durant une session d'un utilisateur de l'ENT, 6 requêtes sont effectuées en moyenne sur le référentiel d'authentification / autorisation : 1 requête d'authentification et 5 requêtes d'autorisation.

La solution proposée par le soumissionnaire devra maintenir un temps de réponse à chacune des requêtes d'authentification / autorisation inférieur à une (1) seconde.

Le soumissionnaire précisera par ailleurs les impacts techniques potentiels en cas de doublement des hypothèses d'accès, les mêmes exigences en termes de performance étant conservées.

[EX-5] Performances sur les requêtes des services de publication

Pour chaque requête des services de publication, la solution proposée par le soumissionnaire devra maintenir un temps de réponse inférieur à deux (2) secondes.

[EX-6] Disponibilité

La durée cumulée d'indisponibilité de la solution d'annuaire est inférieure à 8 heures par an. Cette durée est déterminée, hors maintenance, 7 jours sur 7 et 24 heures sur 24.

Le nombre maximum d'indisponibilités de la solution d'annuaire est de 3 fois par an.

La durée maximale d'une indisponibilité de la solution d'annuaire est de 4 heures. Cette durée est déterminée, hors maintenance, sur les jours ouvrés de 07h00 à 20h00.

[EX-7] Hébergement

Il est prévu d'héberger l'annuaire ENT sur à compléter par la maîtrise d'ouvrage en charge du projet ENT: quel site ? quelles responsabilités pour l'exploitant du site ? quels services d'exploitation sur le site ?...

Certains établissements pourraient cependant souhaiter héberger physiquement les données qui les concernent. Le soumissionnaire précisera quelles adaptations devraient alors être apportées au modèle et à l'architecture afin de prendre en compte ce besoin et quels impacts pourraient en découler. De même, il précisera les moyens d'administration et d'exploitation à mettre en œuvre.

La maîtrise d'ouvrage en charge du projet ENT pourra supprimer ce paragraphe si la possibilité d'hébergement n'est pas offerte aux établissements.

[EX-8] Exigences communes à tout le socle

La solution d'annuaire devra satisfaire aux exigences définies pour l'ensemble du socle ENT.

La maîtrise d'ouvrage en charge du projet ENT pourra compléter ce chapitre avec les exigences qu'elle jugera nécessaires.

8. Organisation et processus types de gestion de l'annuaire ENT

L'objectif de cette partie est de donner aux soumissionnaires une vision détaillée des processus pressentis pour l'annuaire ENT. La solution proposée devra être capable de gérer ces processus et d'intégrer de manière simple (paramétrage et interface graphique) de nouveaux processus du même type et leur déclinaison en workflow.

Ce chapitre ne présente qu'un exemple possible d'organisation.

La maîtrise d'ouvrage en charge du projet ENT devra ainsi préciser les rôles des différents acteurs et les processus de gestion, en s'appuyant le cas échéant sur les propositions ci-dessous.

8.1. Organisation type de la gestion des droits d'accès

8.1.1. Acteurs

L'organisation de la gestion des droits d'accès aux données de l'annuaire ENT peut reposer sur les acteurs présentés ci-dessous.

8.1.1.1. Administrateur central

L'administrateur central de l'annuaire ENT a accès en écriture sur les objets de type « profil applicatif partagé », « rôle applicatif » et « application » transverses à l'ENT.

Il est ainsi en charge de la création de ces objets et de leur mise à jour.

8.1.1.2. Propriétaires et gestionnaires locaux

Le chef d'établissement est le propriétaire de l'ensemble des données sur son périmètre de responsabilité. Les populations concernées correspondent à l'ensemble des personnes rattachées administrativement à l'établissement ou exerçant une fonction dans l'établissement.

Ainsi, le chef d'établissement possède un accès en écriture sur les objets de type « personne », « structure », « profil applicatif local à l'établissement », « rôle applicatif local à l'établissement », « application locale à l'établissement », et peut notamment inscrire une personne dans un profil applicatif.

Il peut déléguer tout ou partie de ses droits sur ces données à des gestionnaires locaux (par exemple, les personnels administratifs).

8.1.2. Définition des droits d'accès

Les articles 4 des arrêtés du 30/11/2006 et du 06/12/2007 relatifs aux ENT définissent les principes de gestion des droits d'accès aux données de l'annuaire ENT respectivement pour le MEN et pour le ministère en charge de l'Agriculture.. Les recommandations pour la déclinaison de ces principes sont présentées à l'annexe 2.

8.2. Processus type de gestion

8.2.1. Gestion des personnes

8.2.1.1. Inscription d'une personne

Plusieurs modes d'inscription d'une personne dans l'annuaire ENT peuvent être envisagés.

Inscription automatique

La création d'une personne dans l'annuaire ENT est réalisée automatiquement depuis les sources d'alimentation. Si une entrée est identifiée comme nouvelle dans la source alors qu'elle est déjà présente dans l'annuaire ENT, une anomalie est déclenchée.

Inscription manuelle par la structure de rattachement

Pour les catégories de personnes qui ne sont pas alimentées automatiquement, la création est réalisée manuellement dans l'annuaire ENT via l'interface de gestion de contenu prévue à cet effet (cf. service [SRV-5]). Cette alimentation manuelle est réalisée par le propriétaire ou par un gestionnaire délégué, en charge de l'établissement de rattachement administratif de la personne à créer.

Inscription individuelle

L'inscription individuelle consiste en une demande engagée par la personne auprès d'un gestionnaire de l'établissement ou du propriétaire, au travers d'un *workflow* où la personne renseigne les informations nécessaires à sa création dans l'annuaire ENT. Une fois ces informations validées par le gestionnaire, la personne est créée dans l'annuaire.

La maîtrise d'ouvrage en charge du projet ENT adaptera ou complétera éventuellement les modes d'inscription proposés en fonction de ses attentes.

Quel que soit le mode d'inscription, l'activation du compte est réalisée à la première connexion de la personne, sous réserve de son acceptation explicite.

8.2.1.2. Suppression d'une personne

La maîtrise d'ouvrage en charge du projet ENT doit préciser ici les actions à effectuer lorsqu'une personne est supprimée du référentiel source. Ces actions peuvent dépendre des catégories de personnes concernées.

Exemples : suppression directe de l'entrée, suspension de l'entrée et suppression automatique au bout d'une durée déterminée, conservation de l'entrée pendant quelques mois puis suppression (permet aux utilisateurs de disposer des ressources pendant quelques mois supplémentaires, notamment afin de récupérer leurs données).

8.2.1.3. Modification d'une personne

Les modifications des attributs d'une personne suivent les modes d'inscription envisageables pour la personne, à savoir une modification automatique via l'alimentation depuis des référentiels externes, une modification manuelle sur demande de l'utilisateur et réalisée soit directement par lui-même, soit par le gestionnaire, ou une modification manuelle réalisée directement par le gestionnaire.

8.2.2. Gestion des structures

8.2.2.1. Ajout d'une structure

La création d'une structure est réalisée automatiquement pour toutes les nouvelles entrées des sources d'alimentation autoritaires.

Pour les catégories de structures qui ne sont pas alimentées automatiquement, la création est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-5]). Cette alimentation manuelle pourra être réalisée par le propriétaire ou un gestionnaire délégué.

8.2.2.2. Suppression d'une structure

La maîtrise d'ouvrage en charge du projet ENT doit préciser ici les actions à effectuer lorsqu'une structure est supprimée d'un référentiel source. Ces actions peuvent dépendre des catégories de structures concernées.

Exemples : suppression directe de l'entrée, suspension de l'entrée et suppression automatique au bout d'une durée déterminée, conservation de l'entrée pendant quelques mois puis suppression (permet aux utilisateurs de cette structure de disposer des ressources pendant quelques mois supplémentaires, notamment afin de récupérer leurs données).

8.2.3. Gestion des profils applicatifs

8.2.3.1. Ajout d'un profil

La création des profils applicatifs est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement créer des profils applicatifs locaux sur son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut créer des profils applicatifs partagés, dont la portée sera transverse à tout l'ENT.

Remarque : L'ajout d'un profil applicatif partagé n'a de sens que s'il est réellement partagé pour tous les établissements d'un projet ENT.

8.2.3.2. Suppression d'un profil applicatif

La suppression des profils applicatifs est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement supprimer des profils applicatifs locaux à son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut supprimer des profils applicatifs partagés, dont la portée est transverse à tout l'ENT.

8.2.3.3. Peuplement / dépeuplement manuel d'un profil

Le peuplement des profils applicatifs est réalisé manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-9]).

Un propriétaire ou un gestionnaire délégué peut uniquement peupler un profil applicatif avec des personnes appartenant à son périmètre de responsabilité. Il pourra peupler tout profil applicatif partagé et tout profil applicatif local à son périmètre de responsabilité.

Le dépeuplement d'un profil applicatif suit les mêmes règles que le peuplement.

8.2.4. Gestion des applications et des rôles applicatifs

8.2.4.1. Ajout d'une application ou d'un rôle applicatif

La création d'une application ou d'un rôle applicatif est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. services [SRV-10] et [SRV-11]).

Un propriétaire ou un gestionnaire délégué peut uniquement créer des applications et des rôles applicatifs locaux sur son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut créer des applications et des rôles applicatifs transverses à tout l'ENT.

8.2.4.2. Suppression d'une application ou d'un rôle applicatif

La suppression d'une application ou d'un rôle applicatif est réalisée manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. services [SRV-10] et [SRV-11]).

Un propriétaire ou un gestionnaire délégué peut uniquement supprimer des applications et des rôles applicatifs locaux à son périmètre de responsabilité.

L'administrateur central de l'annuaire ENT peut supprimer des applications ou des rôles applicatifs transverses à tout l'ENT.

Remarque : La suppression d'une application entraîne la suppression de tous les rôles applicatifs associés à cette application, si le rôle applicatif est uniquement associé à cette application. Dans le cas contraire, seule la référence de cette application est supprimée au niveau du rôle applicatif (attribut « owner »).

8.2.4.3. Peuplement / dépeuplement manuel d'un rôle applicatif

Le peuplement d'un rôle applicatif est réalisé manuellement dans l'annuaire ENT via l'interface prévue à cet effet (cf. service [SRV-10]).

Un propriétaire ou un gestionnaire délégué peut uniquement peupler un rôle applicatif avec des personnes ou des profils applicatifs appartenant à son périmètre de responsabilité. Il pourra peupler tout rôle applicatif associé à une application transverse ou locale à son périmètre de responsabilité.

Le dépeuplement d'un rôle applicatif suit les mêmes règles que le peuplement.